

EXHIBIT 126



TECH

Q&A: How safe is private browsing?

Kim Komando, Special for USA TODAY

Published 7:30 a.m. ET Feb. 15, 2013

Key Points

Private mode forces browser to ignore cookies%2C browser history

Free ebooks available on Project Gutenberg%2C Feedbooks

Sell handmade crafts on Etsy%2C ArtFire

You've got tech questions, here are the answers. Kim Komando helps you make the most of your technology by answering your thorniest tech questions. So if you're wondering what to buy, how to plug it in, or how to fix it, Kim can help.

How private is private browsing?

Q. I saw that my browser has a private browsing function. Does this actually keep people from seeing what I'm doing?

A. That depends on who you're trying to hide it from. Private or Incognito browsing can be turned on in most browsers by hitting CTRL+SHIFT+P (CTRL+OPTION+P on Macs). The major exception is Chrome, where it's CTRL+SHIFT+N (OPTION+SHIFT+N). Private mode forces your browser to ignore cookies and doesn't record your browsing to your browser's history. **It's good for hiding your browsing from snoops and people who use your computer.** However, ad trackers can still sniff out your information, and your ISP still records where you go. If you want to try to avoid that, you need to use a proxy, like KProxy . Don't mistake either of these as an excuse to do anything illegal.

Download thousands of free ebooks

Q. I'm joining a book club. We read a new book every week, so I need to find a way to save money on books. Would using ebooks help?

A. They sure could! You can actually find thousands of free ebooks on sites like Project Gutenberg and Feedbooks. You don't even need an ereader to read them — any smartphone, tablet or computer will work. The one catch is that you won't find many recently released books on free ebook sites, which might be what your book club is focused on. For that, try Overdrive. It's an app that cruises your local library for ebook loans of more recent titles. You can check out books right from the app, and it returns them for you automatically.

Detect and remove spying software

Q. I read recently that people can use something called a keylogger to spy on me. What is a keylogger? How do I tell if I have one?

A. A keylogger is a hardware gadget or software program that monitors everything you type and creates a log of it for someone else. Some keyloggers can take photos of your screen, too. Keyloggers are good at hiding, so you need a special program to find them. KL-Detector usually does the trick. If it finds a keylogger, you can try to remove it with your security software, but you'll usually need a paid program like SpyReveal. Note that hardware keyloggers can't be detected with software. However, hardware keyloggers usually plug into an open port on your computer or attach to your keyboard or mouse connections, so you can find it just by looking.

Speed up your PC with more RAM?

Q. My computer is starting to slow down. Will more RAM speed it back up?

A. It could under the right circumstances. If you have an older computer with less than 4 gigabytes of RAM, doubling the current amount of RAM will make it snappier. Use the Crucial scanner to see what kind of RAM your computer supports. However, if you already have 4 GB or more, adding more won't help your cause. In that case, you want to check with a program like Process Explorer to see what programs are taxing your system. It should give you a good idea of what is slowing things down. Keep in mind that a virus could be the cause, so make sure you run a scan with your anti-virus of choice.

Open up shop online

Q. I have a small business and I'd like to start selling my products online. What tools can I use?

A. Most Web hosting companies have business plans for less than \$10 a month. Almost all of them include built-in e-commerce systems. If you don't already have a site, look into hosting from Bluehost, DreamHost or HostGator. The only problem with these sites is that you have to construct the store yourself. You might want to look into specialty services like Shopify, Magento Go or Amazon Webstore. These do much of the work for you. If you're selling handmade things, it might be easier to sell them on an arts-and-crafts shop like ArtFire or Etsy.

Kim Komando hosts the nation's largest talk radio show about consumer electronics, computers and the Internet. To get the podcast, watch the show or find the station nearest you, visit www.komando.com. E-mail her at techcomments@usatoday.com.

EXHIBIT 127

The Washington Post
Democracy Dies in Darkness

We've all practically given up on Internet privacy. Here's how not to.

By [Brian Fung](#)

September 5, 2013 at 9:26 a.m. EDT

Now that we know the NSA is watching our every move online, it seems almost pointless to try and avoid it. But try we do, as a new Pew Research Center survey shows.

Eighty-six percent of U.S. Internet users have used some method to cover their tracks online. Problem is, even as solid majorities say people should be able to surf the Web anonymously, not many of us are confident that that's possible. Just 37 percent of U.S. Web users say complete anonymity can ever be achieved.

The good news is that there's a big gap between people's expectations and what most have already tried.

Cache-clearing and cookie-disabling is a fairly common behavior. But for whatever reason — inconvenience, maybe, or unfamiliarity with the tools — the share of Americans that have tried protecting their privacy in other ways is pretty low.

So what can be done? Here are a few options that don't involve cracking open a computer science textbook.

Encrypt your e-mail. This is by far the scariest-sounding technique, but if you have a set of step-by-step instructions, you'll be up and running in no time. The basic idea is that for every e-mail account you own, you can create a set of public and private keys that will turn your plain-text e-mails into unreadable gibberish.

Encrypt your chats. Instead of using Google Talk or AOL Instant Messenger, try switching to a chat application that supports encryption out-of-the-box. A lot of people on Windows prefer Pidgin (the Mac analogue is called Adium). Illustrated instructions for setting up your first encrypted chat can be found [here](#) (Windows) and [here](#) (Mac).

Enable incognito mode on your Web browser. Most browsers come with an private browsing or incognito mode that won't log your search or browsing history and won't retain cookies that sites use to track your behavior. While it won't encrypt the traffic you send over the networks, it's a good way to hide your activity from others who might use the same computer later.

Use a traffic anonymizing service like Tor. Tor routes your traffic through the Web in ways that makes it very hard for someone else to track. When the service is turned on, your Internet traffic looks to outsiders like it's coming from one of Tor's exit relays, which can be located anywhere in the world (read: not where you are). You can download Tor [here](#).

Pay for a private VPN. This option is a lot like using Tor in that your Internet traffic is masked, but depending on your provider, it could come with more features. For the privacy-conscious, [TorrentFreak](#) quizzed a number of VPN providers on how they operated their business and only listed those that returned satisfactory answers.

Use a password manager. Part of the point of encrypting your Internet traffic is to reduce the likelihood of someone gaining the passwords to your online accounts. So why not beef up the security of those accounts in the first place? As Microsoft's Troy Hunt writes, the strongest password is the one you can't remember. To help you keep track of them all — and you'll have a lot, if every password is different — use a password manager like LastPass or 1Password. Browser extensions, integration with Dropbox, mobile versions and strong-password generators are all examples of features that help make these tools less of a burden and more useful.

EXHIBIT 128

Is Chrome's Incognito Mode Really Private? 4 Things to Know About it

KHAMOSH PATHAK (<https://www.guidingtech.com/author/kpathak/>) 10 Oct 2014



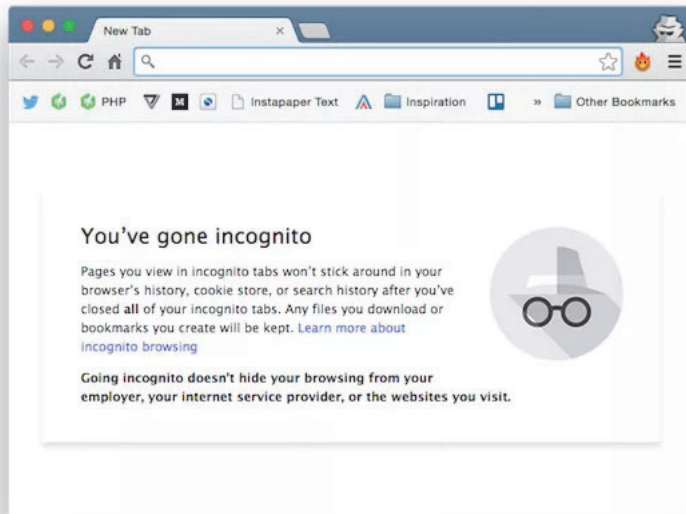
Many internet users think that [incognito mode in Google Chrome](https://www.guidingtech.com/11757/instantly-switch-chrome-tab-to-incognito-private-mode/) (<https://www.guidingtech.com/11757/instantly-switch-chrome-tab-to-incognito-private-mode/>) is like a magical cloak that will instantly gives them internet privacy. That's just not true.



Incognito mode gets a bad rep. Some say it's only used to hide "indecent" behavior. But there are legitimate uses for it. What is incognito mode? Just how "private" is it? Why even use it? And is there anything better to keep your affairs private on the internet? All of your questions will be answered below.

1. IT'S NOT REALLY PRIVATE

Well, **nothing** really is private these days but if you're thinking that switching to incognito mode is going to magically cloak your internet behavior, you're wrong.



When you switch to the incognito tab, Chrome itself tells you, “Going incognito **doesn’t** hide your browsing from your employer, your internet service provider, or the websites you visit.”

Yup. Your internet service provider still has a list of all the websites you visited. The website you’re viewing might also keep a record of your stay. And as Chrome used to say, your browsing habits are never quite protected from the person standing right behind you.

2. IT WON’T SAVE YOU FROM SECRET AGENTS

Before the NSA revelations and the incognito page redesign, Chrome had a funny line in there. Thanks to Dailykos (<http://www.dailykos.com/story/2014/03/04/1282215/-Sh-t-just-got-real-Chrome-Incognito-Description-Trades-Quirky-for-Informative>), we can all enjoy it. Listed under Be wary of was **Surveillance by secret agents**.

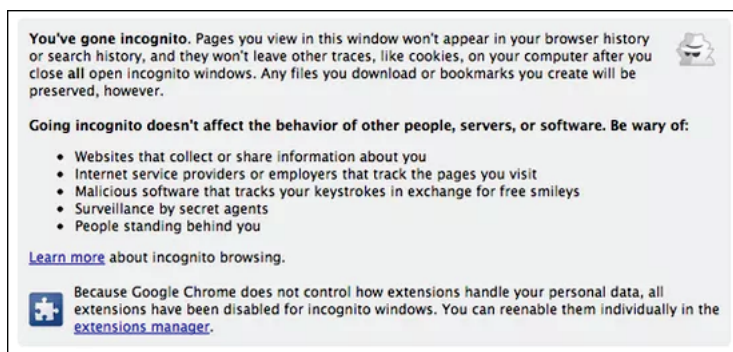


Image capture via Dailykos.

That little joke turned out to be a little too true and was consequently removed from the redesign.

The point I’m trying to make is that when it comes to privacy, incognito mode is certainly not what you should be relying upon.

3. INCOGNITO MODE: WHAT IS IT GOOD FOR?

The point of incognito mode is not to hide your identity from the rest of the world, it's to hide your interactions with the internet from the PC you're using (and the Google account you're logged into).

> **COOL TIP:** If you're letting a friend check their email or log into Facebook on your personal computer, have them do it in a new **INCOGNITO WINDOW** (Ctrl+Shift+N). This way, it's like they're using an entirely different browser – which means they'll log into their accounts without having to log you out first. Everybody wins. They can use your computer without having all of their user information saved in your cookies, and you don't have to relog into all of your sites.

When you use incognito mode, Chrome doesn't record any history or cookies, and it disables browser extensions. This means that third party services like Facebook, Google, etc that use cookies to track your movement across the internet to serve you better ads won't follow you to the incognito tab.

Due to these reasons, incognito mode is generally safer when making banking transactions or having conversations you don't want to be recorded **on your PC**.

When cookies and extensions are disabled, the chances of a malicious app (<https://www.guidingtech.com/33535/block-malware-android/>) stealing your data are largely reduced.

If you use Gmail, Google Search and an Android phone, you know just how obsessive Google's tracking is. Google Now on your phone will follow up on something you searched for on a computer that one time. Incognito mode prevents such encounters.

4. IS THERE A WAY TO TRULY BE PRIVATE ON THE INTERNET?

VPN Maybe

Maybe not "truly" (ahem, secret agents), but we can surely try. Using VPN is usually the easiest and most effective way. A VPN **masks** physical location and IP address. So the website you're visiting doesn't really know who or where you are.

Chrome has two good VPN extensions called ZenMate (<https://chrome.google.com/webstore/detail/zenmate/fdcgdnkidjaadafnichfpabhfomcebme?hl=en>) and Hola (<https://chrome.google.com/webstore/detail/hola-better-internet/gkojfkheleghikafcpjkiklfbnlmeio?hl=en>). I've written about security based extensions on Chrome (<https://www.guidingtech.com/33178/chrome-security-extensions/>), in detail before.

For Windows and mobile devices, Hotspot Shield (<https://www.guidingtech.com/17306/best-vpn-apps-iphone-hotspot-shield-vpn-express/>), and TunnelBear (<https://www.guidingtech.com/15663/tunnelbear-vpn-android-phone-how-to/>), are great VPN services.

But if you really do not want to take any chances when it comes to privacy, you can check out VPN services like NordVPN and ExpressVPN (sign up using this link and save 49% (https://www.xvbelink.com/order?offer=3monthsfree&a_fid=guidingtech&data1=order), on a yearly ExpressVPN plan.)

Use Tor Instead of Chrome

Chrome is built by Google. It is arguably the fastest and most feature rich browser out there. But Google makes money by serving you ads based on your personal information. By using anything from Google you're essentially giving up your privacy.

To a lot of people, that's worth the convenience.

If you really want to say no to Chrome, try Tor as your browser (<https://www.torproject.org/download/download>). It's an open source browser that's designed from the ground up to hide the identity of the user. It works similar to VPN software but on a browser level.

WHAT DO YOU USE THE INCOGNITO MODE FOR?

Let us know what you use incognito mode for in the comments below, but please, don't be indecent!

Top image via Normand Desjardins (<http://www.flickr.com/photos/cafemoka/6681037203/in/photolist-bbo4AB-9ELk7D-9ELiCH-9ELjjK-9ELiYe-9ELjJB-aKX2e-gffgM-6dgtjy-2vBk4-9ELkwt-gfejs-cuvP49-g4YRs-g4YRv-g4YRp-g4YRq-g4YRo-g4YRk-4quomo-aKX2M-aKX2C-bCgVRJ-sEVXw-pxJ3x-8BgKD-7tMvRb-96hYiV-5dYrJT-sEVC8-cuvT2G-sEVCb-sEVXr-sEVXp-sEVXu-sEVXt-sEVXo-aPQBGg-8BgN9-8BgHK-7BCqvw-5m7LKp-a7QPz8-dai9nM-bhVy8k-pxHz6-pxHzg-pxHzi-pxJ3u-pxHzg>).

Last updated on 16 Jun, 2020

The above article may contain affiliate links which help support Guiding Tech. However, it does not affect our editorial integrity. The content remains unbiased and authentic.

EXHIBIT 129

These Are All Good Reasons To Use Incognito Mode

By Pamela J. Hobart
Sep. 17, 2016



As most people who browse the internet have noticed by now, most web browser software prominently offers an "incognito mode" option. What is incognito mode anyways, and what are the reasons to use incognito mode? As a recent Reddit thread reveals, there are more than a few.

To understand why you'd want to use private browsing (known as "incognito mode" on the popular browser Chrome), it's best to first understand how incognito mode works. When you open a browser window in private or incognito mode, the browser stops storing all the various stuff it usually stores about sites as you putter around the information superhighway. Typically, this stored stuff includes things like the site's URL, text you may have typed into the site's forms, and cookies from websites (that enable the browser remember your language preference or save your digital shopping cart, for instance). And, very obviously, when you are not in private browsing mode, the browser logs sites you've visited into your "history" log, along with the date and time of the visit.

Incognito mode doesn't offer complete privacy. Your internet service provider still knows where you've browsed, so while

incognito mode might hide your searches from your mom, it can't really help you hide from the police and their subpoenas. If someone like your employer is monitoring all of its network's activity from a central location, they'll know where you (or your computer) has navigated, too.

But for personal day-to-day purposes, the incognito mode is really valuable. As explained by the good folks on Reddit, here are some of those times.

1. Looking at porn

People who use "Incognito Mode" on your web browser for reasons other than porn, what are those reasons? (self.AskReddit)
submitted 2 days ago by ManofCin
8505 comments share pocket

This very common incognito mode use case is right there in the question! As everyone knows, internet porn is tremendously popular, but sometimes you want to keep your browsing to yourself. Incognito mode is the answer. You can even conveniently use browsers incognito on your phone.

2. Signing into multiple email accounts at once

[-] BookerDeWittsCarbine 6046 points 2 days ago
 Multiple email accounts open without having to sign out of them.
permalink embed pocket

You could set up different browser "profiles" to switch between email accounts within one browser, but incognito mode is the quick and easy way of doing this on the fly — no setup required.

3. Watching weird videos

[-] DMan304 4592 points 2 days ago
 Anything weird I don't want in my history without having to wipe the entire history. Especially on Youtube where it will pollute my whole Youtube environment.
permalink embed pocket

Again, though there is another way to pause videos getting added to your YouTube history (within YouTube settings themselves),

the incognito mode is quick and easy.

4. Using computers that aren't yours

↑ [-] **575r** 6803 points 2 days ago

↓ If I need to sign into a website on someone else's computer, none of my credentials will be saved

[permalink](#) [embed](#) [pocket](#)

If you need to log into your email or your banking account or whatever on a computer away from home, just pop open incognito mode to provide a layer of protection against your passwords or user info being saved to that computer (not totally infallible, that computer could have keystroke logging software on it or something, but it helps).

5. Lame Google searches

↑ [-] **erlnno** 4481 points 2 days ago

↓ I use it to google stupid questions that have obvious answers that I just don't know or to check the meanings of simple words I happened to forget. I don't know why I do it but that's it

[permalink](#) [embed](#) [pocket](#)

Because there's no such thing as a stupid question, except when that old nonsense is staring you down in your autocomplete fields or browser history. Let's send those lame Google searches down the memory hole with incognito mode instead.

6. When you don't want to look like you're up to no good

↑ [-] **CoffeeAndKarma** 972 points 2 days ago

↓ I dabble in art. Sometimes this requires me to look up pictures of children cause drawing from a reference is much easier. But I don't want my search history filled with "12 year old girl" "8 year old boy" etc, for understandable reasons.

[permalink](#) [embed](#) [pocket](#)

↑ [-] **Joliet_Jake_Blues** 1136 points 1 day ago

↓ I saw a "child oral" website in my friend's search history and had a moment of terror/panic

Then I remembered he was in dental school.

Then I saw that the rest of the link was "care".

I gotta tell you, that 1/4 of a second was a roller coaster of emotions.

[permalink](#) [embed](#) [parent](#) [pocket](#)

↑ [-] [saintofhate](#) 265 points 1 day ago

↓ Doing research for writing which includes things such as:

- Best non-fatal place to stab someone
- how to dissolve a body in acid/lye
- best place to shoot someone for slow death
- how to hotwire a car
- do cars explode when shot
- how much trauma can the body take before passing out
- how to make explosives
- how long does it take to die from stomach wound

Some searches just look real bad out of context.

7. Shopping for gifts

↑ [-] [bhare418](#) 2798 points 2 days ago

↓ gift shopping

[permalink](#) [embed](#) [pocket](#)

↑ [-] [wildistherewind](#) 829 points 2 days ago

↓ The one where you buy your SO flowers online, then a week later you bring up a web page to show them something and flower ads are all in the sidebar before the flowers are delivered. Thanks, fuckfaces.

[permalink](#) [embed](#) [parent](#) [pocket](#)

↑ [-] [willem_the_foe](#) 462 points 2 days ago

↓ This happened to me a couple months ago.

My SO bought me a bunch of stuff at REI, where we share a membership. She used the membership card on purchase to get the benefits, a week later (my birthday was two weeks later) I get an email saying "Hey you! Write a review for all your new stuff!"

[permalink](#) [embed](#) [parent](#) [pocket](#)

↑ [-] [RoyalPoodle](#) 200 points 1 day ago

↓ Happened to me for engagement rings! Fucking assholes.

[permalink](#) [embed](#) [parent](#) [pocket](#)

↑ [-] [fletchindr](#) 174 points 1 day ago

↓ 'i was just looking at them, didn't buy any. shes been looking at me weird for weeks and gets mad every time I tie my shoe. then I saw the fucking adsense about rings...'

[permalink](#) [embed](#) [parent](#) [pocket](#)

Big Data has no reservations about spoiling a surprise. Or "spoiling" a surprise that it not actually about to happen, as it were.

8. Because it's prettier

↑ [-] [WillTheLittle](#) 1544 points 2 days ago

↓ I use the 'private' setting on iPhone safari just because I like the dark colour scheme

[permalink](#) [embed](#) [pocket](#)

Ok sure, if you say so!

EXHIBIT 130

GOOGLE APPS MOBILE

Google's iOS app now lets you lock incognito searches behind Touch ID

By Jacob Kastrenakes | @jake_k | Sep 27, 2016, 3:00pm EDT | 7 comments



Justin Sullivan/Getty Images

Google will now let you privately search the web in its core app on iOS. The ability to search in incognito mode is being added in an update to [the Google app](#) that's coming out today.

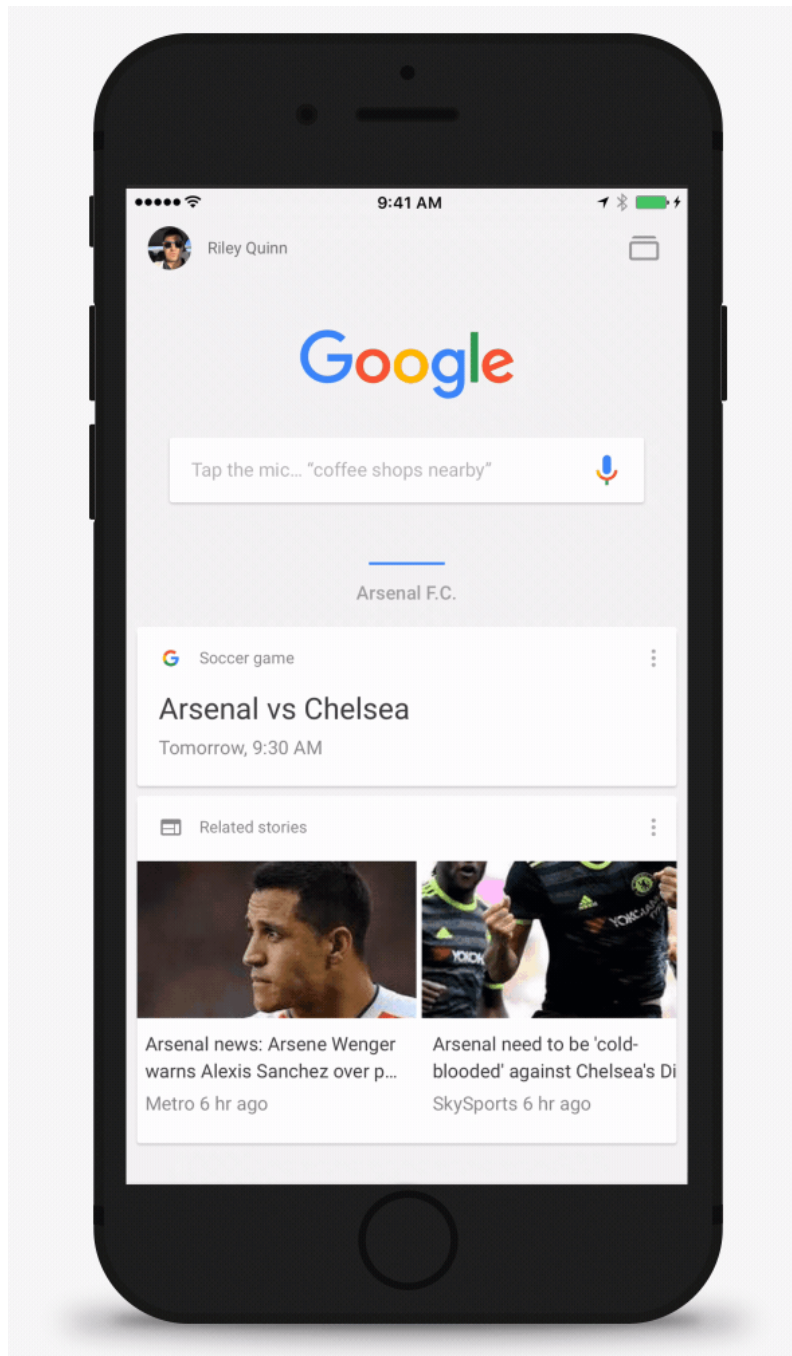
But the more interesting part of the update isn't incognito mode on its own — private searches are already available in both Chrome and Safari, so that's nothing new — it's how Google is making them even more secure. Google will let you lock up private searches using Touch ID, so that if someone else is holding your unlocked phone or tablet, they won't be able to see private tabs that are still open inside the app.

MAKING PRIVATE MODE A BIT MORE PRIVATE

It's a small but helpful change. Ostensibly for convenience, Google doesn't close private searches when you leave its app — you have to manually close them yourself. By requiring Touch ID authorization to see those searches again, Google is able to protect against one of the reasons people might have been using a private search in the first place: family and friends seeing what they've been up to.

All that said, it's worth remembering that Google's incognito mode isn't perfectly private. As Chrome warns you when you open a private tab, "Going incognito doesn't hide your browsing from your employer, your internet service provider, or the websites you visit." In the case of the Google app, it won't hide your searches from Google, either — it just won't tie them to your account.

In addition to incognito mode, today's update also includes the ability to watch YouTube videos directly in the app.



Google

EXHIBIT 131

THE PROBLEM SOLVER

By Michael Connell, Computerworld
APR 4, 2017 10:42 AM PDT

OPINION

You are not very incognito in incognito mode

If you are concerned about your online privacy, you should know what incognito mode does and doesn't do to protect it.

Modern browsers offer an increased privacy option that goes by a number of different names: Incognito Mode in Chrome, Private Browsing in Firefox and Opera, InPrivate Browsing in Internet Explorer and Microsoft Edge, and Private Window in Safari. Since all of these do more or less the same thing, so I'll just use Chrome's "Incognito Mode" moniker as shorthand to refer to all of them.

When you open an incognito window in Chrome, the most popular browser choice, there is a description that explains the limits of what is protected from prying eyes. Judging from a number of conversations I've had, this description is often ignored. A surprisingly high percentage of people mistakenly think that going incognito hides their activity from all prying eyes. As Google's description of incognito mode makes clear, this is not the case:

"Pages you view in incognito tabs won't stick around in your browser's history, cookie store, or search history after you've closed all of your incognito tabs. Any files you download or bookmarks you create will be kept."

[Related: Online privacy: Best browsers, settings, and tips]

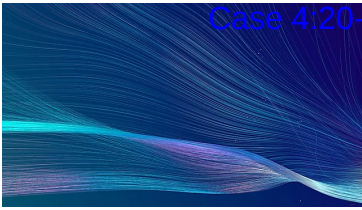
However, you aren't invisible. Going incognito doesn't hide your browsing from your employer, your internet service provider, or the websites you visit."

There are two types of privacy to consider: local privacy and online privacy. Only your local privacy, what people can see on the computer where your browsing takes place, is effected by switching to incognito mode. **Your online privacy is not impacted in any way.**

Basically, incognito mode just means that the browser doesn't save cookies, temporary internet files or your browsing history when you are in incognito mode. The main thing it does is hide your browsing history from other people who use the same computer. Not all of reasons someone might want to do this are nefarious; I used incognito mode when I was shopping for Christmas presents on a shared computer this past year, and successfully managed to keep the gifts I searched for and purchased a secret.

There are other uses for incognito mode apart from keeping your browsing history secure from prying eyes. For example, you can be logged into your main Google account, then open an Incognito Window and use it log into a separate or secondary Google account at the same time. The same is true for other accounts that you might not want tracking your every online move, such as Facebook.

Many users have a mistaken understanding about the limits of what incognito mode can do. Despite the clear warnings offered when opening an incognito tab, some still think that it hides their online activity from everyone, including their ISP or employer, when this is obviously not the case. Perhaps it is the "spy in a fedora" icon that Google uses for incognito mode leads some to this mistaken conclusion, but it does absolutely nothing to keep your ISP or employer from seeing exactly what you are doing online, and this mistake could potentially lead to some embarrassing conversations at the office.



In addition, software that is installed on your computer can also circumvent the privacy protections of going incognito. Parental monitoring software is generally unaffected by incognito mode, for example. Spyware that is installed on a computer may also continue to collect information despite the use of incognito mode.

Incognito mode and other private browsing modes are useful and they do provide a real level of local privacy protection that is easy to take advantage of. As long as users are aware of the limitations and do not expect a magic bullet that completely hides their online activity, it can be a useful tool that is simple to use.

But if you want real online privacy, you are going to have take some extra steps.

Michael Connell a freelance writer who has focused on solving problems for many years, formerly as a trial lawyer and currently by offering solutions to the everyday problems encountered while using current technology. Michael worked as a freelance editor and moderator for both ITworld Answers and IDG Answers.

Follow   

Copyright © 2017 IDG Communications, Inc.

7 inconvenient truths about the hybrid work trend

SHOP TECH PRODUCTS AT AMAZON

SPONSORED LINKS

Online Master of Science in Information Systems at Northwestern University

The data warehouse is overdue for an upgrade – discover the Lakehouse.

Message your employees on Slack with customized security and compliance recommendations for their Linux, Mac, and Windows devices. Try Kolide for 14 days free; no credit card required.

CIS Webinar: Effective Implementation of the CIS Benchmarks & CIS Controls.

Every second counts when it comes to mitigating cyberattacks and resolving network performance issues. NETSCOUT Visibility Without Borders keeps you one step ahead.

Future-Proof Data Management and Get 150% ROI Over 3 Years

AMD Ryzen PRO 6000 processors deliver superb productivity, enterprise-grade security features, and the reliability that businesses demand.

Copyright © 2022 IDG Communications, Inc.

EXHIBIT 132

By Joe McGauley

Published on 11/19/2017 at 12:01 AM



Jason Hoffman/Thrillist

In December 2008, the internet welcomed Google's Incognito Mode, a privacy option for Chrome, with open arms. The feature offered protection against overbearing browser-history snoops at a time when many of us considered getting caught visiting NSFW sites (OK, let's be frank: *porn*) on a computer to be the biggest threat posed by the web. This wasn't exactly the case.

In fact, hiding your unmentionable browsing habits was hardly the reason a crack team of developers at Google made Incognito Mode. Knowing that Incognito Mode is still widely misunderstood, and has somewhat unfairly come to connote shady behavior, we talked to one of the people who built it, Google's Vice President of Chrome, [Darin Fisher](#). Fisher provided a firsthand take on how people should be using it, and what people *shouldn't* be expecting it to do for them.

Incognito Mode will not help you watch porn at work...

Although Incognito Mode has earned a reputation for helping people shield prying eyes from seeing whatever it is they don't want to be caught having looked at, its origins are far from illicit. According to Fisher, Incognito Mode was born in 2008 with the primary intention of making it easier and more convenient for people who share computers to do so without mucking up their devices with another user's cookies -- the temporary or permanent files stored on your computer by websites to help them recognize you and keep track of your preferences.

That said, it was also meant to help people hide behaviors they didn't want loved ones to see. Though, as Fisher describes it, the scenario Google envisioned involves a boyfriend searching for engagement rings who doesn't want his soon-to-be-fiancée -- with whom he shares a computer -- to get any hint that he's about to propose. The Chrome team wanted to provide a tool that would enable people to "pause" their browser from recording its history so people wouldn't have to purge it in its entirety whenever they didn't want to leave a trace -- a move Fisher describes as "destructive" because it prevents your browser from taking advantage of historical data (e.g., cookies) to power future searches, and causes it to slow down.

... in fact, if you're using it that way, your boss can probably still see what you're doing

When you use Incognito Mode, your browsing activity does not get recorded to the physical device you're using. That doesn't mean all of what you do is necessarily invisible to the people you want to keep in the dark. That's because if you browse an unsecure site (one without an "https") people who are on the same network as you could peek at what you're doing, and see the sites you're seeing.

For example, if you log on to your employer's Wi-Fi using Incognito in hopes of getting away with something shady online, a savvy superior could easily watch as you go about your business. As more and more sites opt to more secure "https" domains this is becoming less of an issue, but the fact remains that Incognito Mode will not protect you from snoops in this scenario.



You've gone incognito

Now you can browse privately, and other people who use this device won't see your activity. However, downloads and bookmarks will be saved. [Learn more](#)

Chrome won't save the following information:

- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity might still be visible to:

- Websites you visit
- Your employer or school
- Your internet service provider

Google (Screencap)

Incognito Mode was not designed to protect your privacy

If you want to conceal the fact you're about to propose to your partner by doing some covert ring shopping on Incognito Mode, do it! But if you expect IM to protect you against the many, many privacy pitfalls inherent to browsing the modern-day web, be aware that's not its purpose. In fact, Fisher explained that the Chrome team agonized over what to call IM in the beginning, intentionally steering away from including "privacy" in the name, because it didn't want to oversell its ability.

"When you launch the Incognito tab there's this disclaimer there where we really try to help make it really clear to people that your activity is certainly still visible to the websites you visit and could be visible to your employer, to your school your, and to your ISP [internet service provide] of course," he says.

What Incognito Mode *is* useful for

While its developers intended Incognito Mode to make sharing your computer easier, it's since become a handy tool in a number of other situations. For instance, some old-hat flight deal searchers claim they've found cheaper fares while doing repeat flight searches in IM, so as to prevent airlines from keeping tabs on their activity and freezing or jacking the price.

It's also a good way to protect yourself against potentially sketchy or unsecure sites you casually encounter. Fisher suggests this is actually one of its best uses, and encourages people to right click on hyperlinks in Chrome and launch them by selecting "Open Link in Incognito Window." Also, consider shopping on Amazon in IM if you don't want the site's pesky "similar item" suggestions to follow you everywhere you go.

The bottom line is, be vigilant and keep your browser updated

While Fisher didn't give us his take on how best to browse without leaving any trace whatsoever, and acknowledges that Incognito Mode should not be considered a privacy shield, he maintains that the best way to protect yourself and your privacy in the age of rampant online identity theft and hacking is to make sure you're using a modern browser and keeping it updated. The Chrome team is constantly monitoring threats and bugs, and ensures its updates include patches and fixes to address whatever security breaches people are most at-risk of, he said.

The truth is, the only way to be truly invisible online these days is to use a browser like Tor on the Dark Web. Then again, if you don't know what that is or how to get there, you should probably steer clear -- "Dark" is the word that describes it in more ways than one.

EXHIBIT 133

Google says Chrome's incognito mode was not designed to let people secretly watch porn

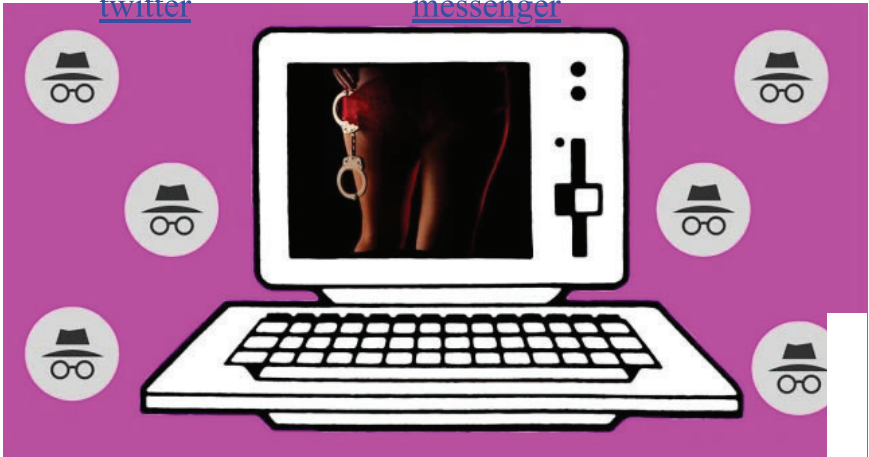
[Comment](#)

 [Jasper Hamill](#)
Monday 20 Nov 2017 4:34 pm

[Share this article via facebook](#)

[Share this article via twitter](#)

[Share this article via messenger](#)



It turns out that incognito mode was not designed to let people watch porn in private (Picture: Google, Getty)

Porn lovers around the world use Google Chrome's incognito mode to hide their tracks when surfing for smut.

But a top Google engineer has claimed this face-saving functionality was actually designed with a much more wholesome purpose in mind.

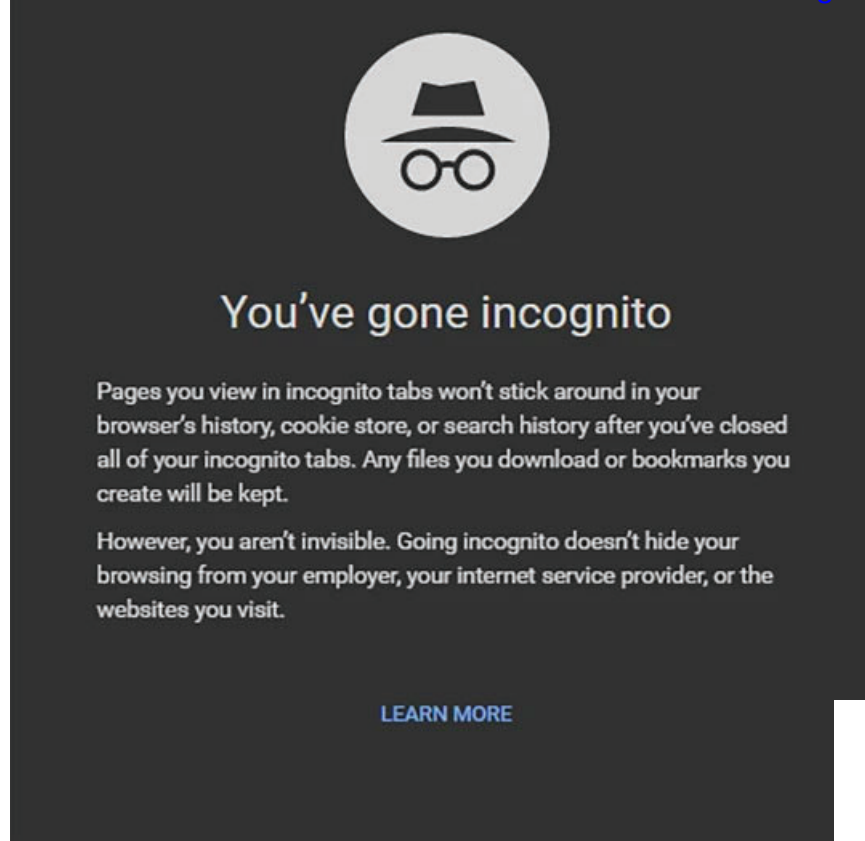


Incognito mode allows people to watch adult content without a record of it being kept in their browser's history.

It's perfect for lusty folk who want to feast their eyes on filthy videos without having to worry about their grubby predilections being exposed.

[Fossilised remains of ancient 'Dragon Death' flying unearthed](#)

Now Darin Fisher, vice president of Chrome at Google, has insisted the incognito option was designed to help people hide a different kind of secret from their partners.



If you see this screen on your partner's computer, they are probably buying a wedding ring. Honest (Credit: Google)

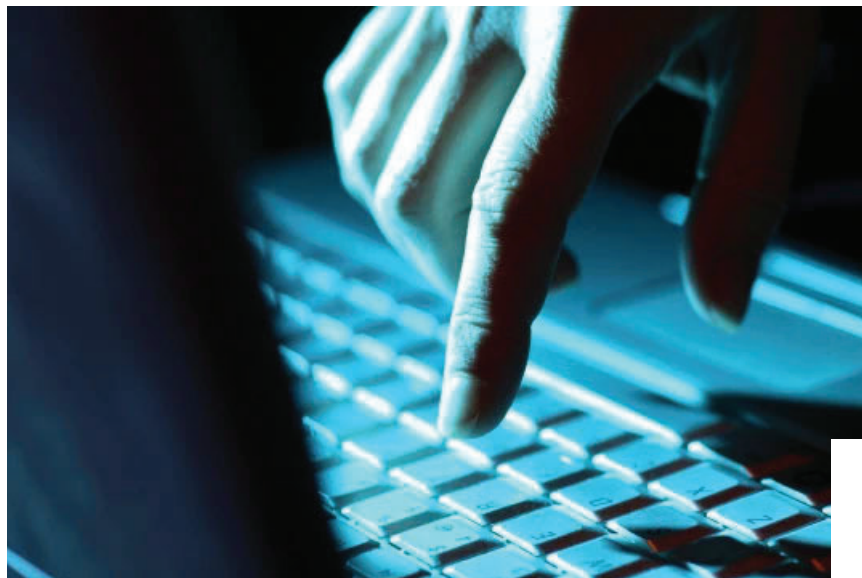
He told Thrillist that Google engineers first imagined it would be used by men who wanted to buy wedding rings without alerting their partner.

The notorious porn mode was intended to let users 'pause' their web activity without having to clear the browser history, he continued.

It was also intended to be useful for people who share computers to use the internet without building up cookies – the name for tiny files downloaded when you visit websites which allow them to remember your preferences and how many times you've visited.

If you believe Google, the fact that it lets porn-pickers hide their tracks was an unintentional quirk of its design.

Fisher also warned users that Chrome could not hide their smutty shame entirely.



Porn fans around the world depend on incognito mode to hide their naughty secrets (Picture: Getty)

Last year, one engineering student claimed that incognito mode failed him by [exposing his porn-watching habits](#).

Another tech expert went one step further and claimed that details of [every website you visit using incognito mode could be accessed and released by hackers](#).

EXHIBIT 134

GUNNED DOWN Google Chrome's incognito mode DOESN'T stop your boss

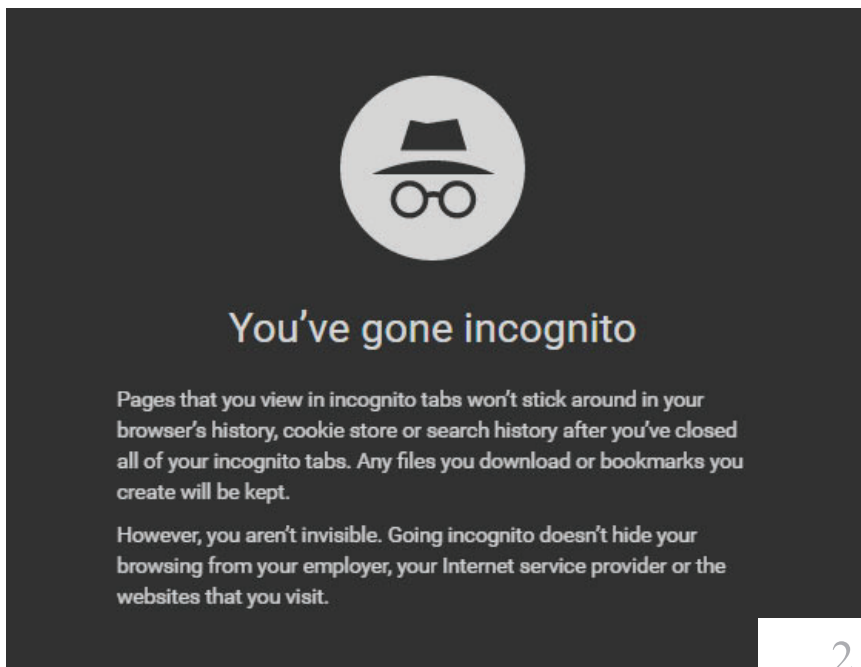
seeing what you're browsing

Alahna Kindred

13:22, 20 Nov 2017 Updated: 14:12, 20 Nov 2017

THINK you can get away with looking at saucy stuff online using Incognito Mode at work? Well think again.

A Google developer has revealed that bosses can still keep tabs on employees' web use on work devices — even if they use the more covert browser.



Google Chrome Incognito Mode can't protect you from eagle-eyed bosses Credit: Google Chrome

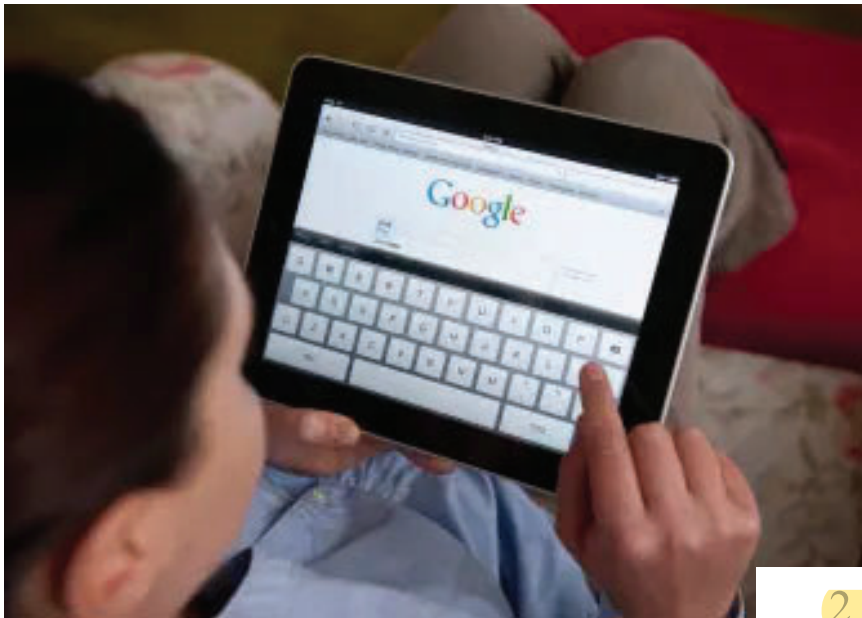
Darin Fisher, who helped create Google Chrome, said [the tech giant](#) "agonised" over naming the secretive tab, which does not save browsing history or cookies.

It is most commonly used to look up blue movies or x-rated snaps without the risk of

being rummled by someone who uses the same device.

But as Mr Fisher explained, they did not want to call it "privacy mode" — as it is not completely private.

He told online mag [Thrillist](#): "When you launch the incognito tab there's this disclaimer there where we really try to help make it really clear to people that your activity is certainly still visible to the websites you visit and could be visible to your employer, to your school, and to your [internet service provider] of course".



2 |

Employers could have access to your browsing history on company devices - even if you use Incognito mode Credit: Getty - Contributor

It means staff could still be hauled up for using company computers to search for blue content even if Chrome's Incognito mode was used.

Users will notice that there is a brief warning when opening the secretive

window which gives a small disclaimer.

It says that your activity "might still be visible to" the websites you visit, "including the ads and resources used on those sites".

It reads: "Pages that you view in incognito tabs won't stick around in your browser's history, cookie store or search history after you've closed all of your incognito tabs.

"Any files you download or bookmarks you create will be kept.

"However, you aren't invisible. Going incognito doesn't hide your browsing from your employer, your Internet service provider or the websites that you visit."

Incognito is instead recommended for avoiding unwanted cookies and keeping web use secret from other users of the same device, Mr Fisher added.

EXHIBIT 135

[independent.co.uk](https://www.independent.co.uk)

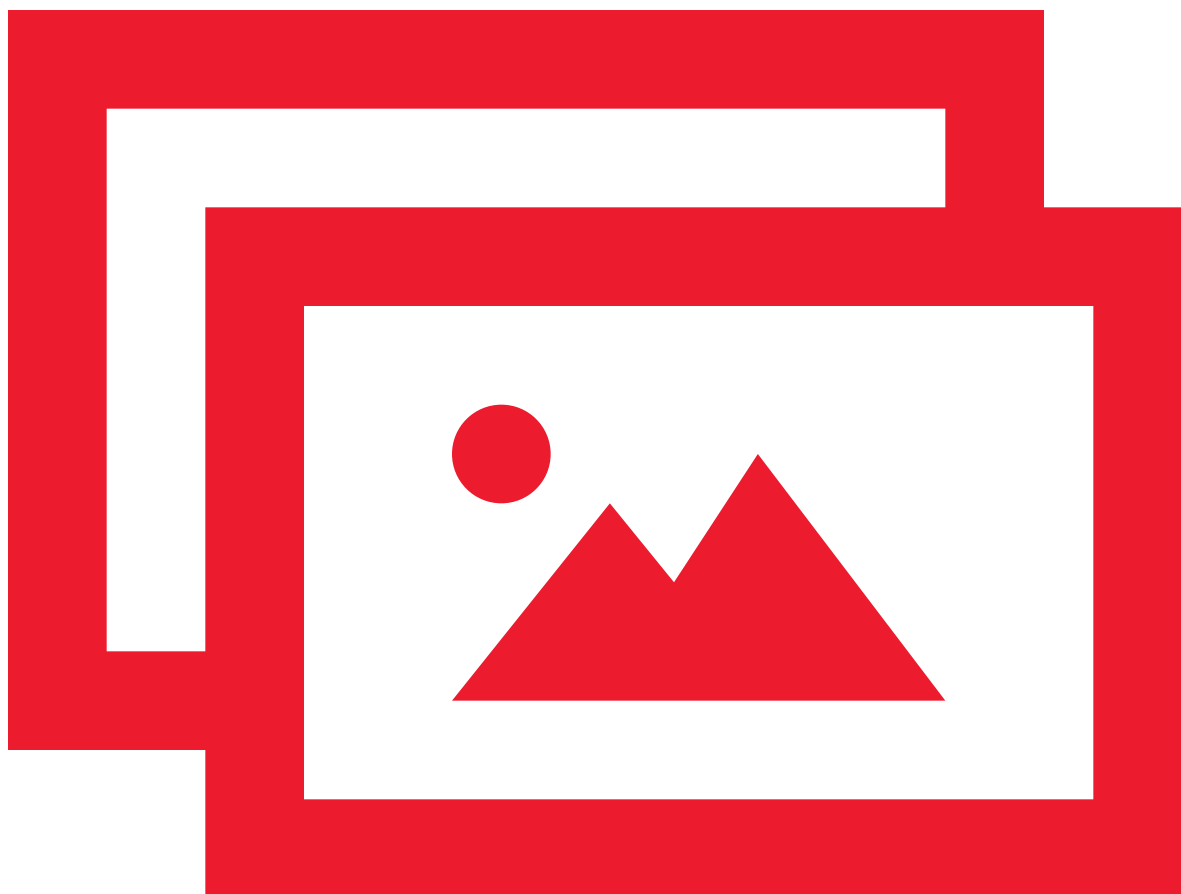
If you use incognito mode, you should read this

2-3 minutes

People can still monitor what you do online even when you use [Google](#) Chrome's incognito mode, a Chrome developer has explained.

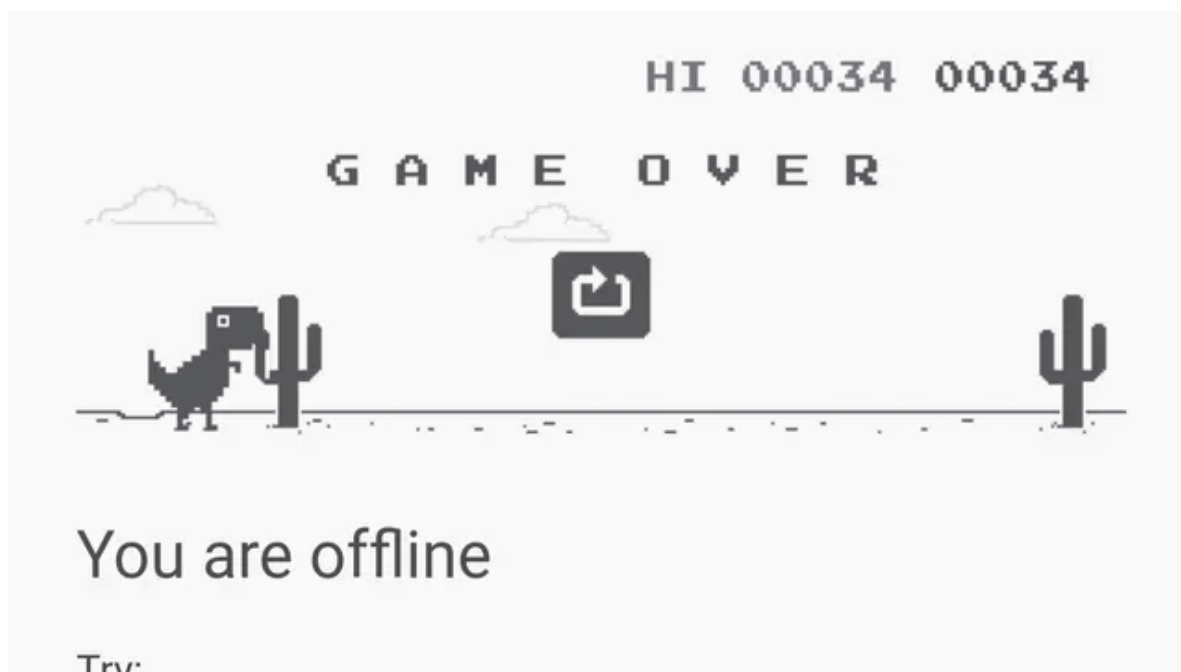
While incognito mode stops Chrome from saving your browsing activities, they could still remain visible to others.

It's bad news for anyone who uses incognito mode to access NSFW content online.



11 hidden Google Chrome features you didn't know existed

Show all 11



According to [Chrome](#) developer Darin Fisher, Google "agonised"

over what to name the feature, deliberately choosing not to call it “privacy mode” in order to avoid misselling it to users.

“When you launch the incognito tab there’s this disclaimer there where we really try to help make it really clear to people that your activity is certainly still visible to the websites you visit and could be visible to your employer, to your school, and to your [internet service provide] of course,” he told [Thrillist](#).

Indeed, whenever you enter incognito mode or open a new incognito mode tab, a short message appears on-screen, briefly explaining how it works.

It says Chrome won’t save your browsing history, cookies and site data, and information entered in forms, when you’re in incognito mode.

However, Google adds that your activity “might still be visible to” websites you visit, “including the ads and resources used on those sites”; your employer, school, or whoever runs the network you’re using; and your internet service provider.

Google reiterates this on its incognito mode help pages, [saying](#), “Your activity isn’t hidden from websites you visit, your employer or school, or your internet service provider.”

Amongst other things, that means your boss could figure out if you’re doing something you’re not supposed to at work, even if you’re browsing incognito.

Mr Fisher instead recommends using incognito mode for avoiding cookies, hiding activities from people who may have access to your computer, such as a loved one you’re buying a present for, and protecting yourself against potentially dodgy websites.

EXHIBIT 136

Google Chrome's Incognito mode isn't 100% private

Your browser doesn't hide your activity from your employer

[VIEW COMMENTS](#)

You've gone incognito

Privacy restriction: Incognito mode on Google Chrome doesn't hide your activity from everyone / Google

By [Ben Travis](#)

28 November 2017

Just when you thought you could make your browser history entirely private, a Google developer is here with some bad news: you're not totally off the grid when you're using Chrome's Incognito mode.

The browser setting can be turned on to ensure your PC or phone doesn't collect cookies or leave a record of the URLs you visit.

However, that doesn't mean that your browsing history is totally hidden.

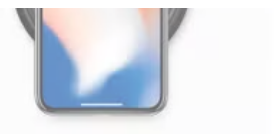
Speaking to Thrillist, Google's Vice President of Chrome, Darin Fisher, explained what Incognito actually does – and warned people about what it can't do.

"When you launch the Incognito tab there's this disclaimer there where we really try to help make it really clear to people that your activity is certainly still visible to the websites you visit and could be visible to your employer, to your school your, and to your ISP [internet service provider] of course," he said.

He added that Google struggled to come up with a name for Incognito that didn't oversell the limited privacy that the mode provides.

iPhone X - In Pictures





This might not be totally new to all users – as Fisher notes, the abilities and limits of Incognito are spelled out for users who open the mode.

“Now you can browse privately, and other people who use this device won’t see your activity. However, downloads and bookmarks will be saved,” Google’s warning reads.

“Chrome won’t save the following information: Your browsing history, cookies and site data, and information entered in forms.

READ MORE

Should Google Pixel 2 XL’s screen problems put you off?

Samsung Galaxy X bendable phone hinted on official website

Samsung mocks the iPhone X and Apple fans in Galaxy advert

Promoted Stories

Gronk's Favorite "Dressy" Shoes Feel Like Walking On Clouds

WOLF & SHEPHERD

Sponsored Links by Taboola

“Your activity might still be visible to: Websites you visit, your employer or school, your internet service provider.”

Fisher suggests users go Incognito when they’re buying gifts online for loved ones who use shared devices, or to protect against dodgy websites that collect user data.

MORE ABOUT

GOOGLE

GOOGLE CHROME

EXHIBIT 137

Contribute →

News website of the year

News Opinion Sport Culture Lifestyle

Opinion

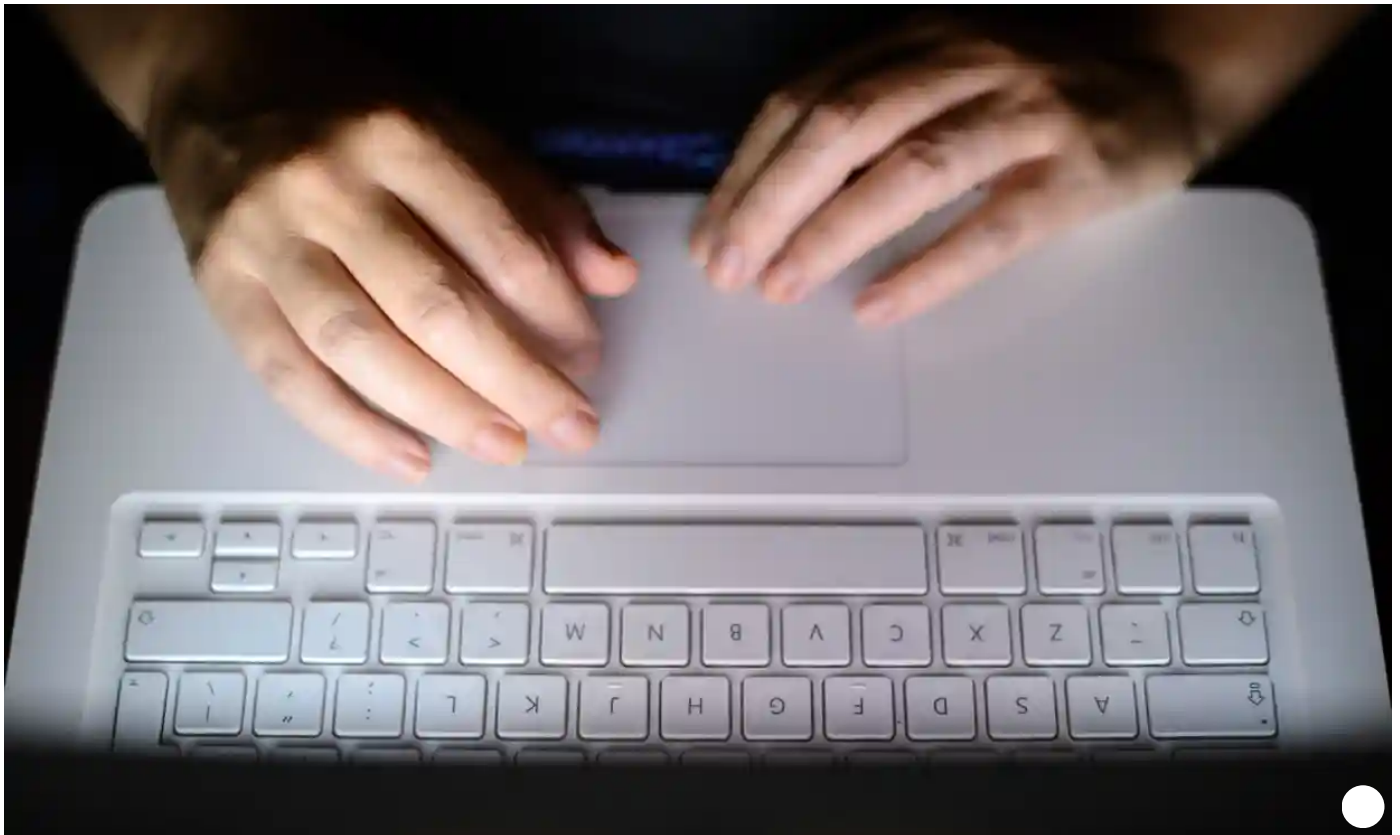
● This article is more than 4 years old

Browsing porn in incognito mode isn't nearly as private as you think

Dylan Curran

When you use incognito mode, it doesn't mean that your activity disappears forever - it's just hidden on the incriminating device

Sun 27 May 2018 11.33 EDT



Ctrl-shift-N: the wondrous keyboard shortcut to start an incognito tab in Google Chrome. You hesitantly type in your odious search, and find the porn site which in that moment you feel a magnetizing attraction to.

You pore over the endless volumes of pornographic videos. Image after image promises to delight the senses. You continue scrolling and clicking until you find the video that will satisfy that seductive and overpowering urge.

Then - once the confidential and intimate act is complete - you sit for a serene moment. Phase three of the operation begins. Like the mafia calling in a “cleaning” crew, you discreetly dispose of the evidence and inspect your surroundings for any witnesses.

You close the incognito tab, the proof of your activities disappearing into the ether of the internet. No one is the wiser. Except - that activity doesn’t really disappear.

It’s easy to see why people would think that history disappears the second you close the window.

“Now you can browse privately, and other people who use this device won’t see this activity”, explains Google.

That’s the key: other people who use this device can’t see the activity. That doesn’t mean that *no one* can see the activity, only someone using the incriminating device.

Incognito works in this way: imagine you buy a new phone. You then go on to call and text your friends and family. Then you factory reset your phone.

Your calls and texts won’t appear on *your* phone, but they will still definitely appear on your friends and family’s phones. Through the factory reset, you have just deleted the information on your phone, nothing else.

▲ People clear their search history and caches and think this information just disappears

Typically, you are signed into your Google account when you perform Google searches. People clear their search history and caches and think this information just disappears.

What most people don’t know is that your activity on Google is logged to something called **Google - My Activity**. This shows all of your account history, including all your searches and the websites you’ve visited (**among other things**).

But let’s say you’re smart enough to log out of Google before searching for porn. What most people don’t realize is that portions of pages you’ve loaded are stored as temporary files (or a cache). So now you have to get rid of that, too.

Now for the fun. If you’re super paranoid (like you should be), let’s say you search for porn on your computer, then factory wipe your computer. And you don’t just wipe it once, you wipe it, then use it for another while, then wipe it again, and so forth.

There’s still a trail. Your ISP tracks all the websites you visit, and everything you download or watch. Tracking you straight to your home.

So the way around that, would be to use a VPN (virtual private network). This reroutes your traffic to come from someone else’s server and also to encrypt the information.

Except ... the VPN you’re connecting to *also* tracks what you’re doing, and has evidence of your searches and visited websites. With the right letter from law enforcement, your browsing history could be handed out like free samples at Walmart.

So law enforcement could compromise your porn habits (or almost anything you do) if they have reason to, but at least they’d do it for the greater good of keeping us safe, right? But a few other parties also have access to that information.

Let’s use PornHub as an example. **They market themselves as a company which prioritizes your privacy**, so they should be squeaky clean, and **as a child company of MindGeek which owns over 80% of online porn traffic**, they’re a pretty good example.

From the second you hit PornHub’s home page, they slap you with a “Hot Porn Videos in [insert your country]”. For a website that doesn’t track you, it’s funny that they immediately show you that they know exactly where you are.

Now to the trackers. PornHub only has three, which is actually extraordinarily low for a website which is entirely dependent on advertising. For context, YouTube has around 20 on average when you click on a video.

DoublePimp and TrafficJunky are both adult advertising networks, and when you click on a video, you’re not only sending PornHub your request, you’re also sending your information to these advertisers. The network may notice you prefer gay porn, for instance, and tailor your ads based off of this. They’ll get your IP address, your user agent (this is your browser, your location,

basic PC details, etc) and some other useful information like how much time you spend on certain videos and what categories you like to go through.

I can't comment on these networks' security, but it's important to know that your browsing habits on porn sites are sent to advertising networks like these.

As for Google Analytics, they capture incredibly specific information about you such as all of the above info, your device, your age, your demographic, your IP address, how fast your internet connection is.

PornHub may not technically track you, but their advertisers and Google can tie all of that information to your personal identity. Even more so, if you're signed into your Google account on Google Chrome. But we trust Google to never use that information in a troubling way ... right?

Dylan Curran is a Data Consultant and Web Developer, who does extensive research into spreading technical awareness and improving digital etiquette

... we have a small favour to ask. Tens of millions have placed their trust in the Guardian's fearless journalism since we started publishing 200 years ago, turning to us in moments of crisis, uncertainty, solidarity and hope. More than 1.5 million supporters, from 180 countries, now power us financially - keeping us open to all, and fiercely independent.

Unlike many others, the Guardian has no shareholders and no billionaire owner. Just the determination and passion to deliver high-impact global reporting, always free from commercial or political influence. Reporting like this is vital for democracy, for fairness and to demand better from the powerful.

And we provide all this for free, for everyone to read. We do this because we believe in information equality. Greater numbers of people can keep track of the events shaping our world, understand their impact on people and communities, and become inspired to take meaningful action. Millions can benefit from open access to quality, truthful news, regardless of their ability to pay for it.

Every contribution, however big or small, powers our journalism and sustains our future. **Support the Guardian from as little as \$1 - it only takes a minute. If you can, please consider supporting us with a regular amount each month. Thank you.**

Single	Monthly	Annual
\$7 per month	\$20 per month	Other

Continue →

Remind me in September

VISA



EXHIBIT 138

There are a lot of misconceptions about browsing the web in 'incognito' mode, researchers say



Todd Haselton

July 12, 2018



In this article:

GOOGL
-1.34% ☆

- Researchers found that there are misconceptions about what's actually protected when you're browsing the web in incognito or private mode.
- People believed that ISPs, employers and the government couldn't see what they were doing, when it's possible they can.
- They also thought browsing in private mode would prevent against malware or viruses.

Browsing the web in incognito mode isn't as private as most people think.

Researchers with the University of Chicago and the Leibniz University of Hanover recently published the results of a study that included 450 participants. It found that many participants thought "incognito mode" or "private mode" in a web browser protected their online activity much more than it does.

If you're unfamiliar with private or incognito mode, here's a bit of background: typically, browsers suggest that using that option, which is accessible through the menu bar on most modern web browsers, won't track some of what you do online.

Google's Chrome web browser, for example, says that it doesn't save your browsing history, cookies and site data or information entered into forms. This doesn't mean that data — such as the websites you visit — isn't available to your school, employer or internet provider. Google warns as much when you start using incognito mode.

Despite this, lots of people seem to believe these options in web browsers can do much more than they actually do.

Here are some of the misconceptions highlighted in the report:

- "46.5% of participants 'believed bookmarks saved in private mode would not persist in later sessions,' when they actually do.
- "40.2% of participants thought websites would not be able to estimate a user's location," while in private mode. You can make it harder to estimate your location if you use a VPN .
- "27.1% of participants believed private mode offered more protection against viruses and malware than standard [mode.]" This is a misconception since any files you download and open on your computer could still be infected with malware or viruses.
- "22.0%, 37.0%, and 22.6% of participants mistakenly believed that ISPs, employers, and the government would be unable to track them when they used private mode." If you're on someone's network, chances are they can see what you're doing.

The study also suggests that 56.3% of participants incorrectly believed that browsing in private mode would hide your search history, since Google could still log a user's search and save a copy of that query online, not necessarily on your computer. I tried to replicate this in Chrome and found that a search for "How tall is Shaquille O'Neal?" wasn't logged by Google or on my local computer.

If anything, the research shows that there are a lot of misconceptions about what's logged and what isn't when you're using incognito or private mode on a browser. It's probably safe to assume that what you're viewing online can be found or viewed by others, especially if you're on a work or school network or downloading files.

EXHIBIT 139

Research Busts Popular Myths About Incognito Mode

Two Clicks Is All It Takes

Download Capital One Shopping on your computer — It's free for everyone.

Capital One Shopping

Open

The incognito, or more familiarly known as the private mode, is a feature in most of the modern web browsers and mobile apps, allowing users to use the internet more privately, without recording history in the device being used.

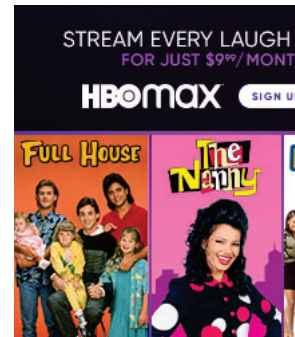
However, in a **research** conducted by the University of Chicago and the Leibniz University of Hanover, with a sample size of 450 participants, **it was discovered that people incorrectly assumed that incognito mode was capable of doing much more than what it can actually do. Even though browsers, like Google Chrome, clearly mention that schools/employers/Internet providers can still have data on browsing history, people tend to ignore this warning quite easily.**

Following are some of the things people think private surfing does:

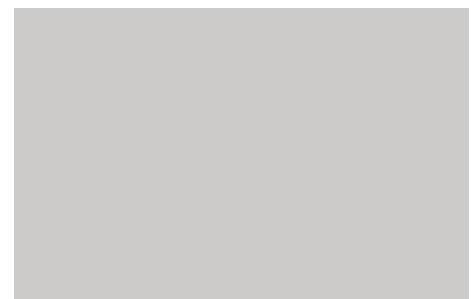
1. Bookmarks saved in private mode do not persist after the mode is turned off.
2. The users location cannot be estimated by authorities (this can be done by using a VPN)
3. Incognito provides protection against malware and viruses present in downloaded content.
4. Governments/Internet providers cannot see what one has been doing online.

As for the last point, there was a huge population which believed in it, when actually this is the most misinformed. **A copy of browsing data is not stored on one's desktop, true; but, reconstructing history, especially by digital forensics experts is not difficult.**

This research can serve as an eye-opener for many people, who believe that they have sound understanding of whatever technology/tools they use in their daily routines.



RECOMMENDED POST



Apple Safari Browser's Bookmarks Are Now Even More Secure, Here's How



Unknown Monday, July 16, 2018



At 7/16/2018 03:49:00 PM

Labels: browser history incognito neha-zaidi news Tech Technology
web-apps

NO COMMENTS:

Post a Comment

Comment as: Google Accour ▼

Publish Preview

< NEWER POST

HOME

OLDER POST >

Google Chrome Is Working On A 'Journeys' Feature, Along With A Sidebar To View A Page And Search Results Simultaneously

Google Chrome to change some of its options and outlooks, giving its browser a more native (Microsoft Edge inspired) look to align its UI with the launch of Windows 11 soon

Google Chrome warns you before downloading any files in incognito mode acknowledging them to be visible to anyone who shares your device

Google's new updated Chrome 94 will be making its way sooner than we expected

EXHIBIT 140

HIDING IN PLAIN SIGHT Google's Incognito Mode not as private as you think

after MAJOR loophole revealed

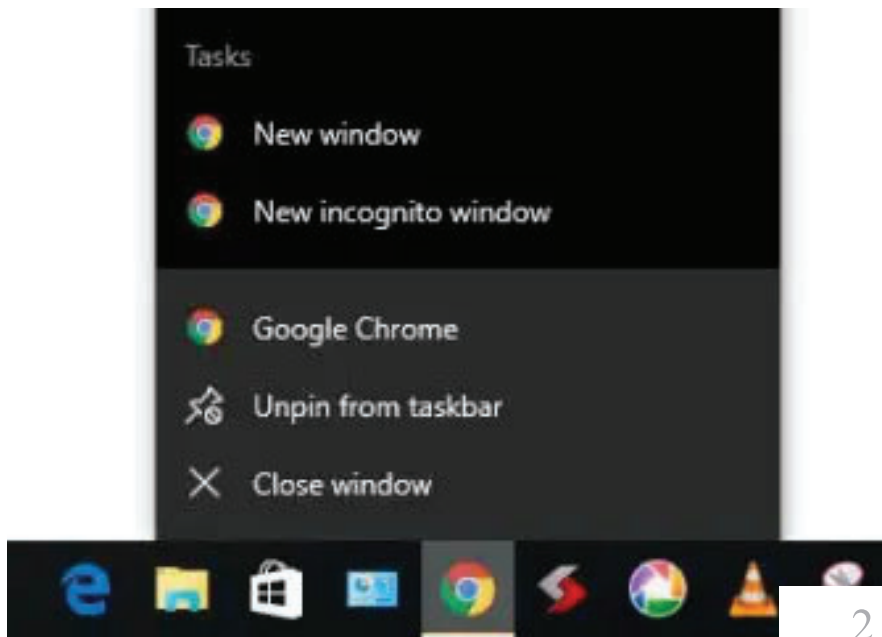
The ultra-private web browser setting has a major loophole that lets Google snoop on your online activity

Sean Keach

11:40, 22 Aug 2018 Updated: 9:30, 23 Aug 2018

GOOGLE'S Incognito Mode is a great way to hide your online antics – but there's a big hole that could leave you exposed.

A new study from Vanderbilt University reveals a sneaky way Google can see exactly what you've been looking at online.



2

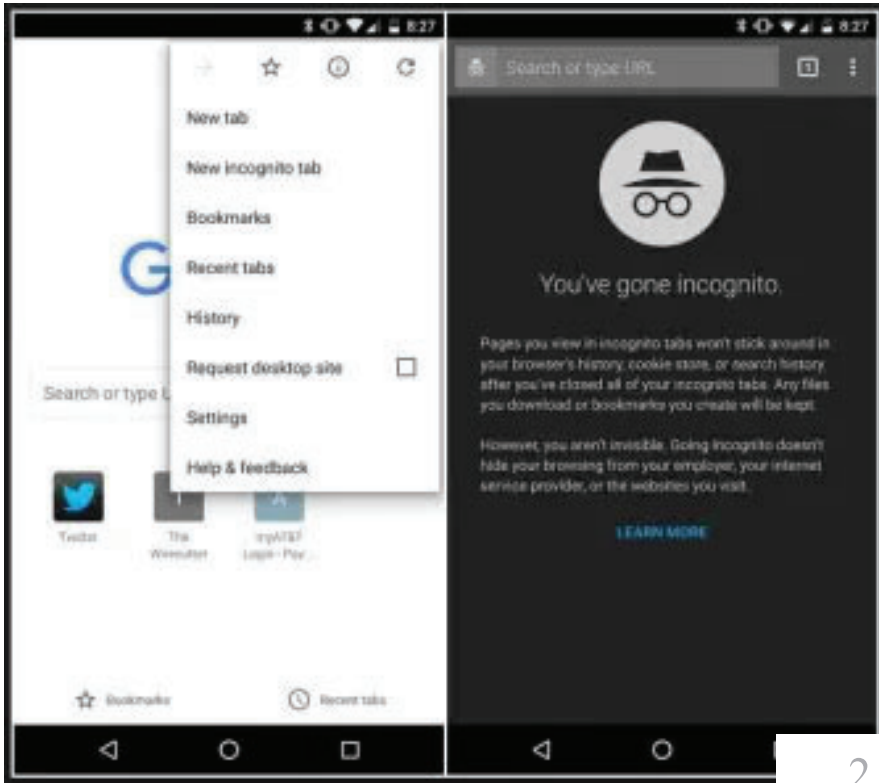
Incognito Mode is a setting in the Google Chrome web browser

The study investigated how Google collects info from you across devices (like Android or Chromebooks) and services (like Google, YouTube, and the Chrome web browser).

And it revealed something very surprising about [Incognito Mode](#).

It emerged that Google can still record the websites you browse while in Incognito Mode on the Chrome browser, and link them to your identity.

This will come as a surprise to some users who thought the special setting protected them.



2

When you're in Incognito Mode, your online browsing activity won't be saved to your computer

Incognito Mode is a setting on Chrome that prevents your web history from being stored.

It also won't store cookies – small files about you – that are linked to your identity.

If you're logged into Google, then what you do online can be traced back to your personal account.

But if you switch Incognito Mode on, you'll only receive "anonymous" cookies, and Google won't be able to link your identity to your browsing habits.

Sadly, there's a catch.

If you log back into Google *before* leaving Incognito Mode, Google will be able to retroactively link your browsing data to your account.

That means Google could see information from before you logged in, but while you were in Incognito Mode – and link it to your Google identity.

This works by taking the previously anonymous cookies, and then associating them with your Google account.

The only way to get around this would be to only log into your Google account after you've left Incognito Mode.

"While such data is collected with user-anonymous identifiers, Google has the ability to connect this collected information with a user's personal credentials stored in their Google Account," the study explained.

Google Incognito Mode – how does it work?

Here's what you need to know...

Incognito Mode is extremely useful, because it can stop your browser saving information about what you do online to your computer

For instance, any websites you visit while in Incognito Mode won't show up in your browsing history

You also won't store any new cookies linked to your own identity (read our [cookies](#) explainer here) – these are small computer files that let websites know if you've been on their page previously

It also won't save any site data – for instance, if you're logged into a website, you'll be logged out in incognito mode

And information won't be stored for later use in web forms that you fill in

This makes Incognito Mode really useful, particularly if you're trying to hide what you're doing from other people in your household

If you're looking for a birthday present for your partner, using Incognito Mode will mean they won't be able to see what you've been looking at

Or if you want to search for something on the internet, but don't want websites to constantly serve you ads for that product in the future, Incognito Mode

you were interested in an item

Douglas Schmidt, a professor of computer science who authored the study, said the loophole is "not well understood by consumers".

"If you read the fine print on 'incognito' mode, it brings up a whole lot of disclaimers," said Schmidt, as quoted in a report by [AdAge](#).

He said that Google collects "all the information necessary" to connect your browsing to your identity.

"It would give them a relative advantage to anyone else who can't do that correlation," he added.

The news comes just days after Google was exposed for spying on your real-world movements, even if you have its [Location History setting turned off](#).

To stop Google tracking your location, you can [follow our handy guide](#).

As far as Incognito Mode goes, it's also worth mentioning that while Incognito Mode stops Google Chrome from saving your browsing habits on your own computer, it won't protect you from outsiders seeing what you do online.

Google Translate warns of APOCALYPSE in bizarre 'end times' message about the Antichrist

Anyone on your Wi-Fi network could potentially use special spy software to view what you're browsing, regardless of Incognito Mode.

And your employer will be able to use similar technology to see what you're browsing at work, too.

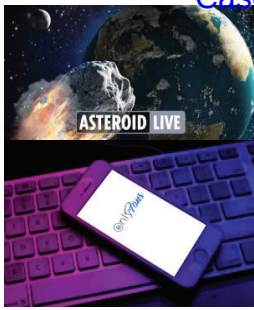
It's entirely possible that your employer logs every website you visit while at work.

Your internet service provider (so BT, Virgin, and so on) will also be able to see what you're doing online.

That means the police can also get access to what you view in Incognito Mode, simply by requesting that information from your internet provider.

The websites you're using will also be able to track that you're online on their page, too.

For instance, Google will know where you're browsing from, and what you're looking at.



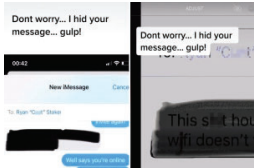
CLOSE UP NASA says 'potentially hazardous'

space rock makes 'close approach' at 29,000mph

FREE FANS How to get OnlyFans for free



MAD SCIENTIST Horrors of Elon Musk's Neuralink REVEALED – including animal deaths



BAD APPLE iPhone warning as horrifying iMessage secret could expose your texts

And if you log into a website, they'll also be able to keep track of information about you.

So when you log into Facebook in Incognito Mode, details about what you do on the site will be recorded – just the same as if you were using it in a normal web browser.

The key point is that Incognito Mode is not a great method of ensuring privacy, because it's still very easy to track what you're doing online.

It's only really useful for keeping websites out of your browsing history, or logging into a single website on multiple accounts in the same web browser.

In a statement, a Google spokesperson said: "This report is commissioned by a professional DC lobbyist group, and written by a witness for Oracle in their ongoing copyright litigation with Google.

"So it's no surprise that it contains wildly misleading information."

Do you trust Incognito Mode? Let us know in the comments!

EXHIBIT 141

How anonymous is DuckDuckGo?



Gabriel Weinberg, CEO & Founder, DuckDuckGo (2008-present)

Updated 1 year ago

If you're unfamiliar with DuckDuckGo, we're the Internet privacy company for everyone who's had enough of hidden online tracking and wants to take back their privacy now. For over a decade, we've built products, created new technology, and worked with policymakers to make online privacy simple and accessible for all. Every day, millions of people rely on our free all-in-one app (private search engine, tracker blocker, mobile browser) to stay private online.

DuckDuckGo search is completely anonymous, in line with our strict privacy policy [↗](#). Each time you search on DuckDuckGo, you have a blank search history, as if you've never been there before.

We simply don't store anything that can tie searches to you personally. In fact, we don't even store anything that could even tie anonymous searches together into an anonymous search *history*, which has been shown in some cases to be able to be de-anonymized (like if you searched for personal information about yourself [↗](#)). That's also why we can't tell you for sure how many people use DuckDuckGo, because if we counted, our users wouldn't necessarily be anonymous. Yes, we take privacy that seriously.

While DuckDuckGo is completely anonymous, Google is of course not. In fact, quite the opposite. On Google, your searches are tracked, mined, and packaged up into a data profile for advertisers to follow you around the Internet through those intrusive, annoying, and ever-present banner ads, via Google's massive [↗](#) ad [↗](#) networks [↗](#), embedded across millions of sites and apps.

Unfortunately, people think that they can make searching Google and browsing the rest of the web anonymous by using Chrome's so-called "Incognito" mode (also known as Private Browsing mode) or its "Do Not Track" browser setting. Sadly, neither of these mechanisms protect you from Google search tracking or its trackers on other websites. We believe it is important to expand a bit on these myths so that you don't have a false sense of security if you choose to utilize those methods.

The Myth of Incognito Mode

A lot of people are shocked to learn that websites can still track you even in Chrome's "Incognito" mode.

The truth is that Chrome's Incognito mode only prevents your browser history from being recorded on your local device and does not offer any additional protection such as preventing the websites you visit from collecting your information (e.g., your searches on a search engine). Check out the fine print [↗](#).

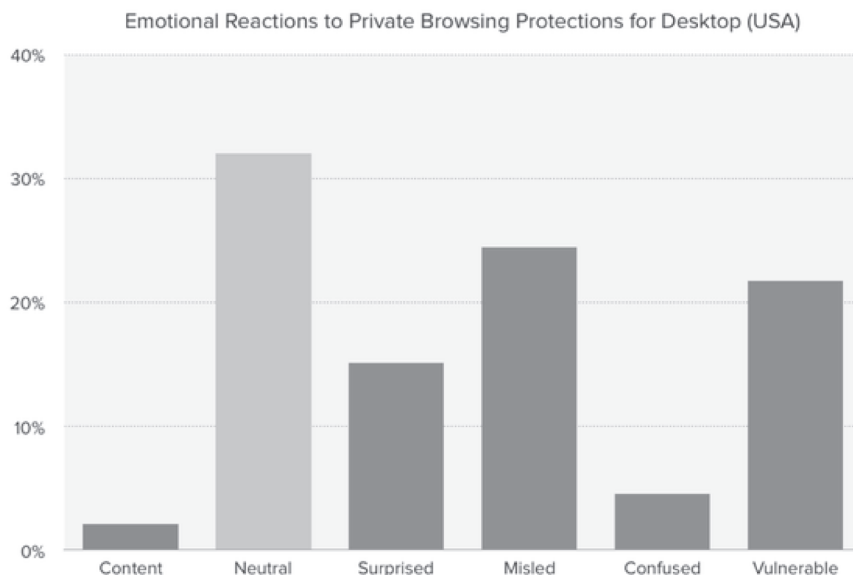
Your activity might still be visible to:

- Websites you visit
- Your employer or school
- Your internet service provider

It is simply a myth that Incognito mode protects your online privacy in any significant way; it is really more of an offline protector. You can easily still be uniquely identified and tracked while using Incognito mode through "browser fingerprinting [↗](#)." Just as each person has a unique fingerprint, so does every browser. Websites can look at your IP address, version numbers of your browser, the plugins it uses, and dozens of other points

That is, while in Incognito mode, Google is still tracking your searches, and can use them to send intrusive ads at you across the Web on the millions of sites and apps that run Google ads. Sure, your search or browser history won't be on your computer, but Google still knows it. And when you get served an ad based on that "incognito" search you did recently (like, let's say that surprise vacation you were planning), it's not so private anymore. On the other hand, DuckDuckGo doesn't track your search history at all, regardless of whether you're "incognito" or not.

We surveyed 5,710 random Americans about Incognito mode to understand what people know about and how they use this common feature. 65% of respondents reported feeling "surprised", "misled," "confused," or "vulnerable" upon learning about the limitations of Incognito mode.

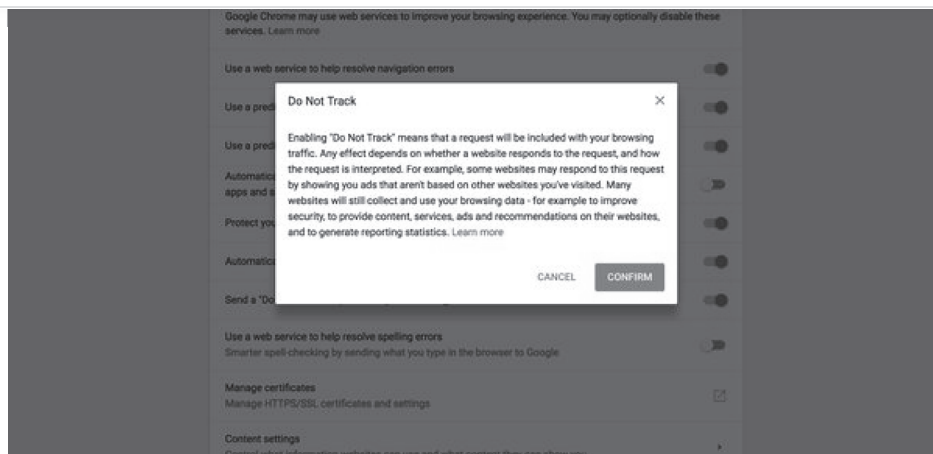


Note that some browsers other than Google's Chrome browser do have private browsing modes that do more to protect you online. Nevertheless, we suggest adding our browser extension [↗](#) to Chrome or other browsers as it blocks more web trackers as you surf the web, helps you use more encryption, and reveals the privacy practices of every website you visit.

The Myth of Do Not Track

In trying to escape Facebook and Google web tracking, you might have turned on the "Do Not Track" browser setting. Unfortunately, it's voluntary and Facebook and Google do not respect it.

Without regulatory measures, the "Do Not Track" setting as it currently stands, is a voluntary setting that hardly anyone respects (including Facebook and Google) which makes it not only ineffective, but worse, misleads people into feeling a false sense of privacy.



Let's Make the Internet More Private

Our mission is to set a new standard of trust online through the privacy tools DuckDuckGo provides – our anonymous search engine at <https://duckduckgo.com> and our apps and extensions that protect your privacy while browsing the web. In one download we deliver privacy, simplified with DuckDuckGo Privacy Essentials on Safari, Firefox, & Chrome and the DuckDuckGo Privacy Browser for iOS or Android today.

Despite increased awareness of privacy issues and actions people can take, there are sadly still many people putting their privacy at risk, or, browsing with a false sense of privacy. This happens for a variety of reasons, including practices such as relying solely on Chrome's "Incognito" mode and Do Not Track setting, as we've detailed here.

To help correct these misconceptions and reach more people, we're also trying to educate users through our blog, social media and a privacy "crash course" newsletter.

The Internet shouldn't feel so creepy and getting the privacy you deserve online should be as simple as closing the blinds.

64.7M views · View upvotes · View 423 shares · Answer requested by Tamara Ortiz, Harvey Eckstein and 2 more

View 35 other answers to this question >

About the Author



Gabriel Weinberg

CEO/Founder DuckDuckGo. Co-author Super Thinking, Traction.



CEO & Founder at DuckDuckGo.com 2008–present



MS in MIT Technology and Policy Program, Massachusetts Institute of Technology Graduated 2005



Lived in Valley Forge, PA



3,953.7M content views 58.9M this month



Top Writer 2018



Published Writer Quora Sessions's Twitter

More answers from Gabriel Weinberg

View more >

How is DuckDuckGo similar or different from TOR?

41,414 views

What key technologies is DuckDuckGo based upon?

8,171 views

If DuckDuckGo is not tracking users, then how do they count user base growth?

197,655 views



What is DuckDuckGo's mission/vision? What role do you hope the company fulfills, in the long-term, on the Internet?

35,511 views

EXHIBIT 142

Google reportedly personalizes search results even when you're in incognito mode



STORY BY
IVAN MEHTA

Ivan covers Big Tech, India, policy, AI, security, platforms, and apps for TNW. That's one heck of a mixed bag. He likes to say "Bleh."

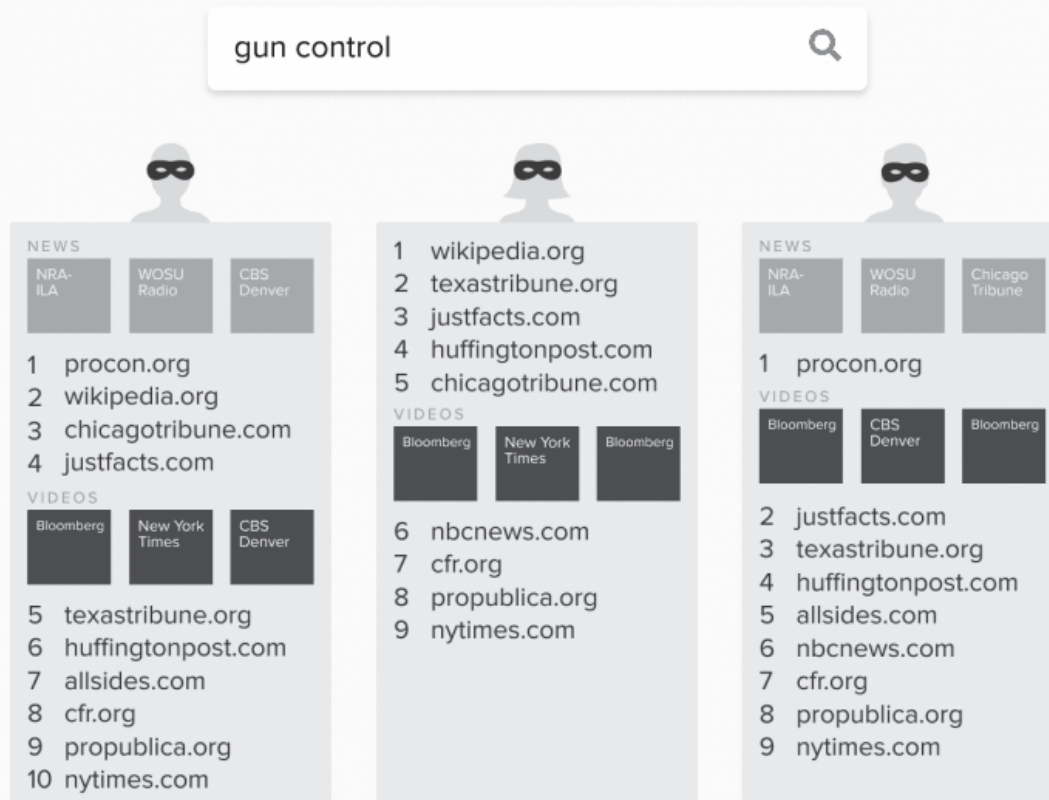
Google provides you personalized search results based on your previous searches, location, and several other factors. So if you want to avoid this and search discreetly without leaving a trail, the most common option is to switch to your browser's incognito mode. However, a new study from privacy-focused search engine DuckDuckGo says that Google search results are uniquely tailored to users, even when they're logged out or browsing in incognito mode.

In the study, participants across the US searched a term at the same time while logged out, or in incognito mode. DuckDuckGo said that logically, the results should be similar, but instead, they were unique to different users.

Google's Filter Bubble

87 people across the U.S. searched Google at the **same time**,
logged out, and in **private browsing mode**.

You might think they would get the same results. **They didn't.**



Actual results from three people in the study.



DuckDuckGo

Credit: DuckDuckGo

The difference of search results for three people for the same keyword in logged out and private browsing mode

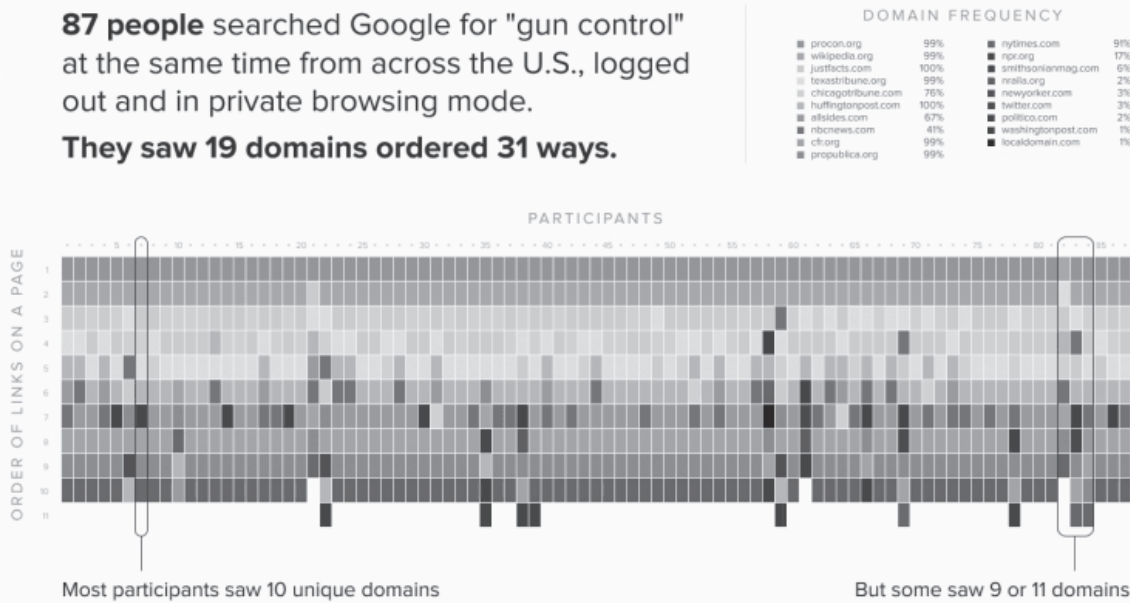
Additionally, links and their orders varied in the news and video infoboxes too. This means some people saw the links other didn't.

That's worrying, because in general, incognito search results should largely be similar for different people, but the variations appear to go beyond that.

Google Filter Bubble Domain Variation

87 people searched Google for "gun control" at the same time from across the U.S., logged out and in private browsing mode.

They saw 19 domains ordered 31 ways.



DuckDuckGo

Study of 87 Americans searching at the same time

The difference of domains in the search results in logged out and private browsing mode

HaVING tROUBLE GROWING yOUR aUDIENCE?

5 omnichannel strategies that actually work

[Read article](#)

DuckDuckGo said that logging out or surfing the incognito mode hardly had any effect on search results:

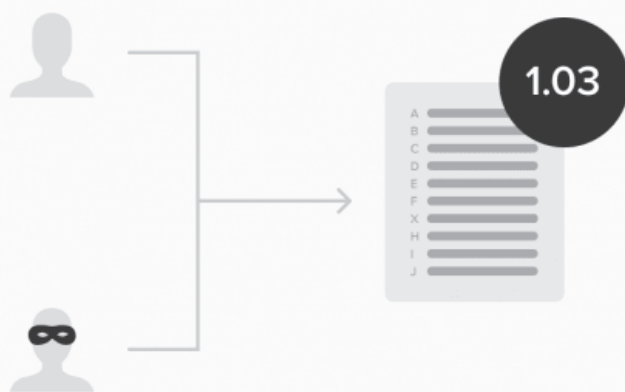
We often hear of confusion that private browsing mode enables anonymity on the web, but this finding demonstrates that Google tailors search results regardless of browsing mode. People should not be lulled into a false sense of security that so-called "incognito" mode makes them anonymous.

Private Browsing and Being Logged Out Does Not Significantly Reduce The Filter Bubble



Variation of Private Browsing Across Users

There are on average **3 domain changes** when comparing two random private browsing mode results.



Variation of Browsing Modes for the Same User

There was on average **1 domain change** for a user in different browsing modes, which suggests **Google maintains the filter bubble within private browsing mode.**



Study of 87 Americans searching at the same time based on "gun control"

Credit: DuckDuckGo

Variation of results for two users in incognito mode and variation of results for the same users in different modes

Google swatted away these claims by saying that the study's methods are faulty:

This study's methodology and conclusions are flawed since they are based on the assumption that any difference in the search results are based on personalization. That is simply not true. In fact, there are a number of factors that can lead to slight differences, including time and location, which this study doesn't appear to have controlled for effectively.

The company wrote a long explainer on why search results may vary for different people, in a series of tweets. Click [here](#) to follow the thread.

Over the years, a myth has developed that Google Search personalizes so much that for the same query, different people might get significantly different results from each other. This isn't the case. Results can differ, but usually for non-personalized reasons. Let's explore...

— Google SearchLiaison (@searchliaison) December 4, 2018

The whole ordeal suggests that it's nearly impossible to get absolutely unbiased search results using Google, as they depend on many factors like time of day and location. While DuckDuckGo's findings shed some light on some of the flaws in Google search results, we

might want to take a competitor's conclusion with a pinch of salt.

You can read the full study [here](#).

Published December 5, 2018 - 6:25 am UTC

EXHIBIT 143

Does Google Chrome have its own VPN?

By James Laird published April 08, 2019

All you need to know...

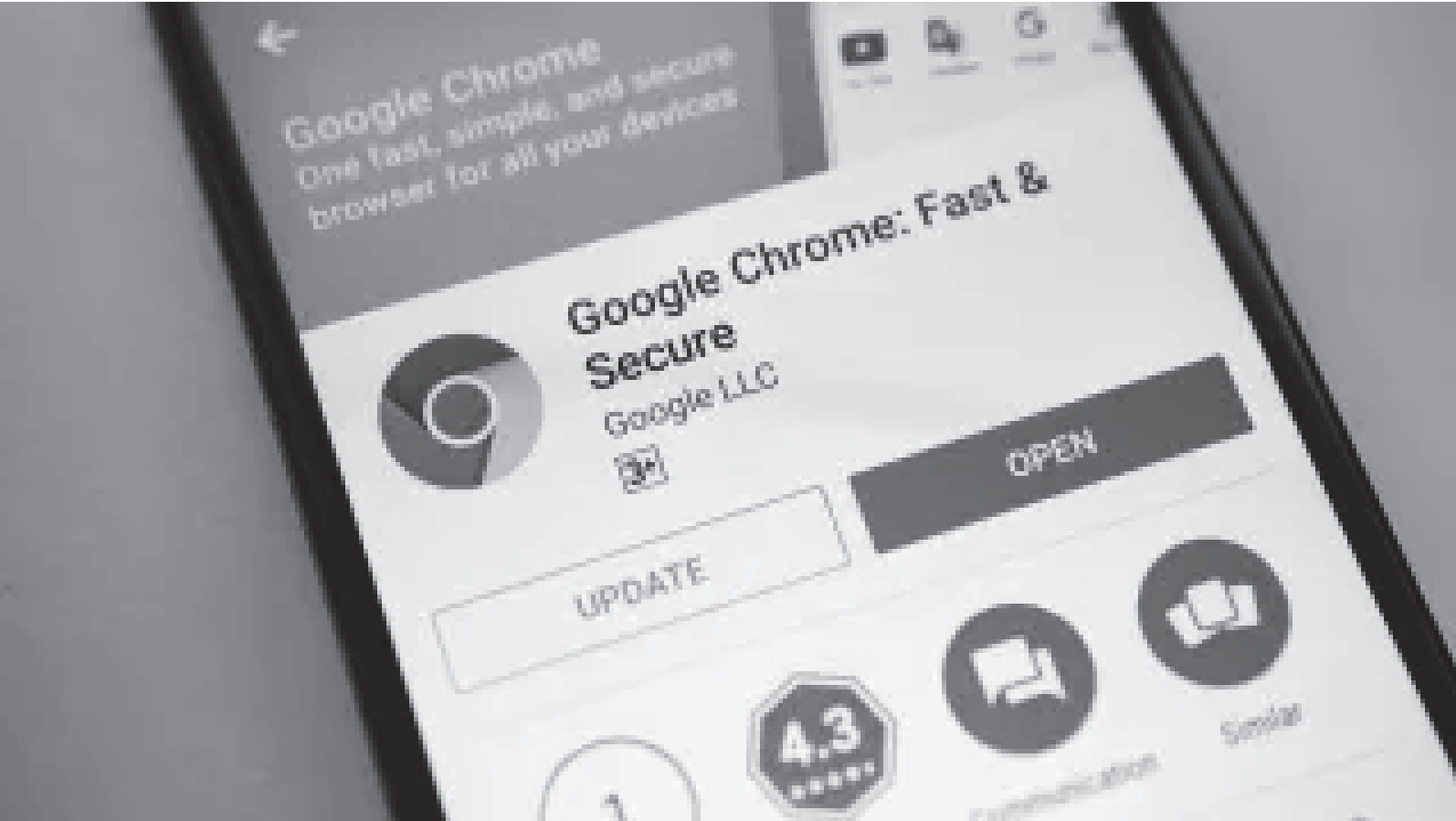


Image credit: Google Chrome (Image credit: Shutterstock)

Google Chrome is the world’s most popular web browser. But despite its near-ubiquity, many users aren’t happy with the way it allows your personal data and online activities to be tracked and, in some cases stored, by advertisers, internet service providers (ISPs) and government agencies. That’s why using a Chrome VPN is highly recommended for privacy-conscious users.

It allows you to use the web truly anonymously, leading many to wonder if Google - like rival browser Opera – offers its own service built-in to its browser.

Does Google Chrome have its own VPN? In short, no.

Sponsored Links

Senior Discounts On TV And Internet In Los Angeles

Senior Cable & Internet Deals



- Discover the very best VPN service
- Are free VPNs safe and can they be trusted?
- Hop straight to our pick of the best Chrome VPN extensions

As with virtually any modern web browser, it does provide a private browsing optic Chrome won’t store your browsing history, cookies, site data, or remember inform.

CLOSE

WILD "Hologram" Technol...

PLAY SOUND



1 of 2. Advertisement

web in this way means that

RECOMMENDED VIDEOS FOR YOU...

However, as soon as you enter Chrome's Incognito Mode, it becomes clear it's not the solution truly privacy-conscious users want. Google immediately warns you that using Incognito Mode in Chrome won't hide your activity from the websites you visit, employers and schools or ISPs.

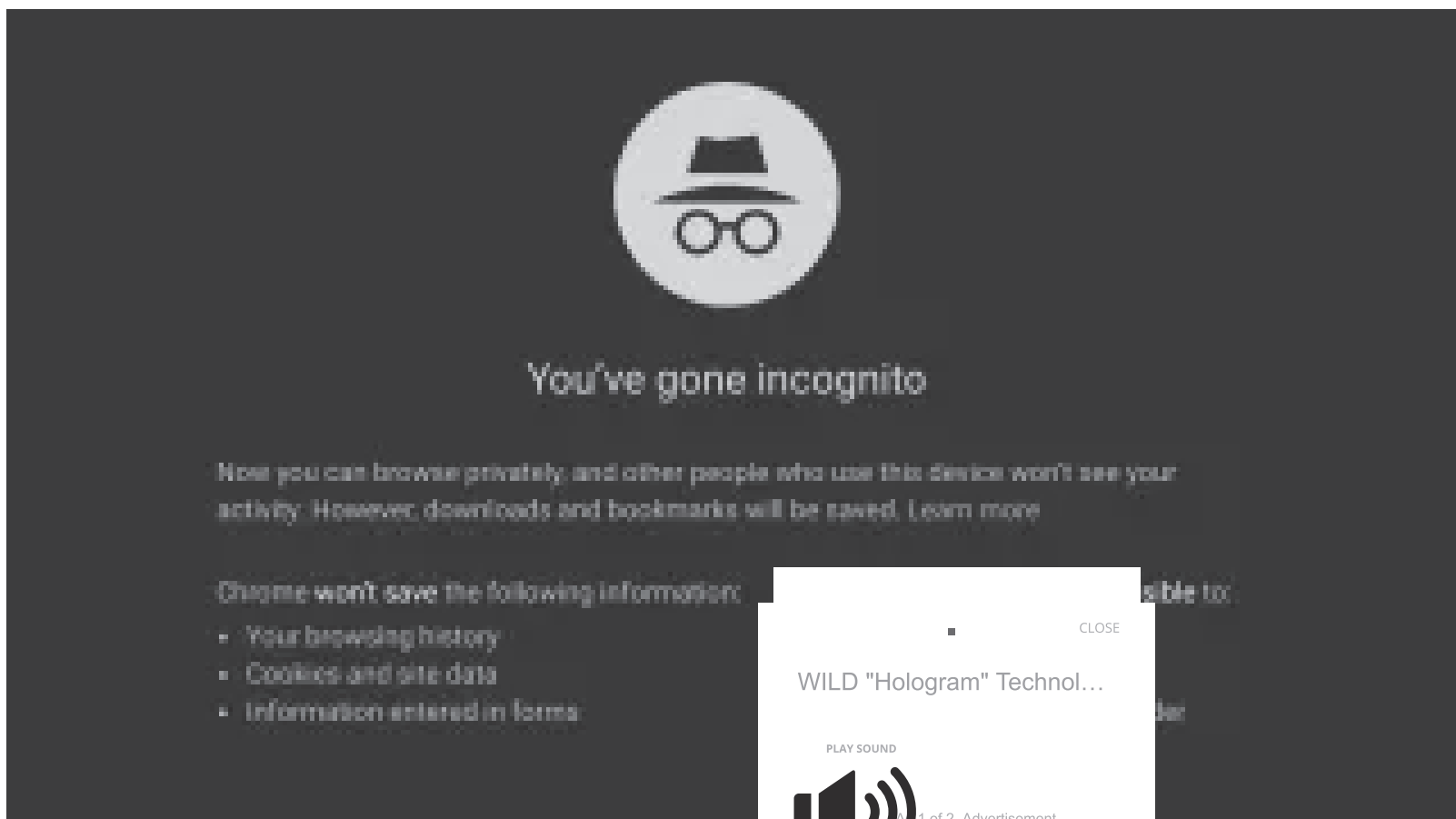


Image credit: Google

This makes it pretty clear that using Incognito Mode is not the same thing as using a Virtual Private Network in full.

Fortunately, while Google doesn't offer its own service, it does support the use of the dedicated best Chrome VPNs through extensions.

Chrome extensions are essentially little applications that you download to your browser, rather than install to your computer proper. They make it easy to access whatever tool you need at a click – without having to leave your computer. We see it's a piece of cake to make something like this.

Installing Chrome extensions is a doddle, so while Google's browser might not offer its own VPN, you have a number of options that can be installed and activated in a matter of minutes.


Our pick of the best extension right now is ExpressVPN, which is affordable (it costs less than \$7 a month when buying a year's subscription), easy to use, and crucially, offers a reliable connection.

Finding the best VPN can seem like a daunting task, given how much noise there is surrounding the subject, but after years of testing various services, Express is the one we recommend right now.


A free VPN can seem tempting as well, but they involve making a number of compromises. In some cases, this might be a daily limit on anonymous browsing time and bandwidth, accepting annoying pop-up ads as you browse, or their server network might just be unreliable and prone to cutting out.

That's why coughing up a small amount for a paid option is a better course of action for the truly privacy-conscious web user. It's a brilliant all-round service that packs all the features you need for anonymous web browsing into an easy-to-use package.

As we've already said, it also crucially offers a handy Chrome extension so you can activate and deactivate it at the click of a button whilst browsing. So while Google Chrome might not have its own VPN, there's no need to worry – ExpressVPN is the next best thing. In fact, based on our experience, it might even be better!

 chrome web store

Home / Extensions / ExpressVPN for Chrome



ExpressVPN for Chrome

Offered by: <https://www.expressvpn.com>

★★★★☆ 333 | Productivity | 5,873,334 users

Add to Chrome

Overview

Reviews

Support

Related

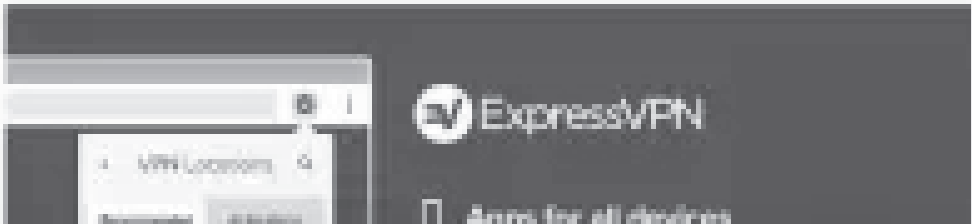



Image credit: ExpressVPN

Should Google Chrome ever introduce its own VPN, we'll update this guide as soon as we get the news. In the meantime, read our full ExpressVPN review to learn more – then check out our guide to enabling a VPN in Chrome to learn how to set yourself up today.

- **Read more:** our guide to the best free VPN
- **Read more:** our guide to the best browsers


CLOSE

 James Laird

James is a technology journalist with nearly 10 years experience and currently Sp TechRadar, T3 and Tom's Guide. He is here to help you find the best ways to watch sports, TV shows and movies online. Previously, he was News and Features Editor at Trusted Reviews, Editor of Lifehacker UK, and Senior Staff Writer at ITProPortal.

WILD "Hologram" Technol...

PLAY SOUND



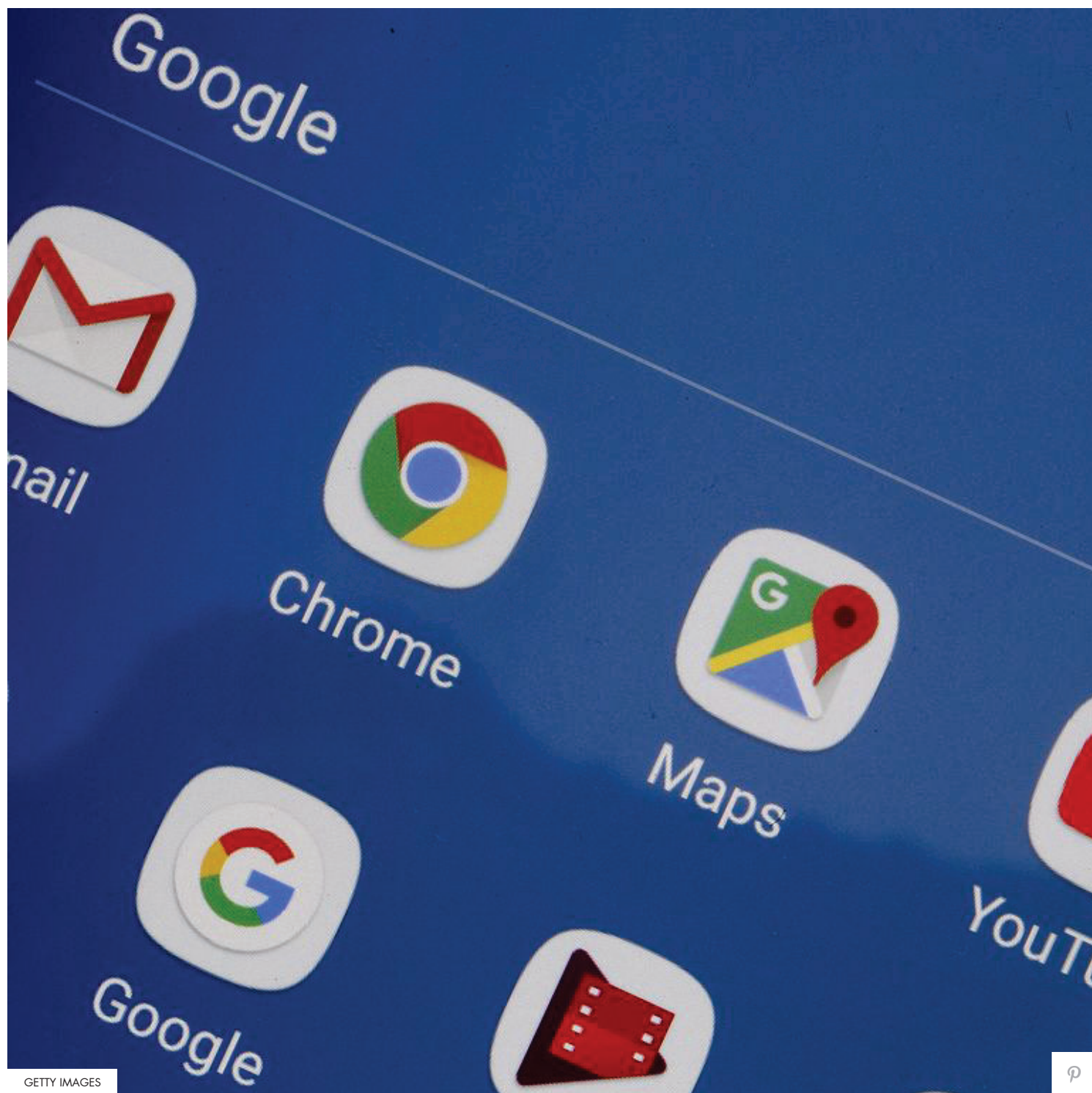
1 of 2. Advertisement

EXHIBIT 144

Sorry, but Google Chrome Incognito isn't as private as you think

Did you know this?

APR 16, 2019



GETTY IMAGES

P

Like everyone, we turn to the internet with our deepest, darkest questions. From 'is my vagina normal?' to 'Can you die from a hangover?', search engines are our best friends when it comes to getting the answers we need.

But if you've ever turned on 'Incognito Mode' in an attempt to hide your searches and hope it helps them stay off the internet, you're going to be in for a bit of a shock.

According to Indy100, 'Incognito Mode' actually only hides traces of your online activity from those using that specific computer, as opposed to the internet as a whole. So while it blocks third-party cookies - and stops your activity ingraining itself into your internet history - it has little effect on your ISP.

more from cosmopolitan

Drag Race UK's Tayce is here to slay



On top of this, 'Incognito Mode' doesn't stop websites being able to follow your activity, meaning that companies can still track wherever you visit on the internet and what you're searching, *even* if you're trying to keep it private.



GOOGLE

A study from Vanderbilt University also revealed that Google can still record the websites you browse while in Incognito Mode on the Chrome browser and link them to your identity, *if* you're logged into your Google account.

ADVERTISEMENT - CONTINUE READING BELOW

"While such data is collected with user-anonymous identifiers, Google has the ability to connect this collected information with a user's personal credentials stored in their Google Account," the study explained.



GETTY IMAGES

There goes any hope of 'privacy', then.

Related Story



You now have to be asked to be in Whatsapp groups

Related Story



Amazon admits staff listen to Alexa conversations

ADVERTISEMENT

MORE FROM

entertainment

The very best hen party houses in the UK

EXHIBIT 145

DAVID NIELD SECURITY JUN 16, 2019 7:00 AM

It's Time to Switch to a Privacy Browser

Ad trackers are out of control. Use a browser that reins them in.



CASEY CHIN

THERE'S A NEW battleground in the browser wars: user privacy. Firefox just made its Enhanced Tracking Protection a default feature, Apple continues to pile privacy-focused features into its Safari browser, and people are more aware than ever before of the sort of information they can reveal every time they set a digital footprint on the web.

If you want to push back against online tracking, you've got several options to pick from when choosing a default browser. These are the browsers that put user privacy high on the list of their priorities.

DuckDuckGo (Android, iOS, browser extension)

You might know DuckDuckGo as the anti-Google search engine, but it's also branched out to make its own mobile browsers for Android and iOS. Not only do they keep you better protected online, they give you plenty of information about what they're blocking.

DuckDuckGo starts by enforcing encrypted HTTPS connections when websites offer them, and then gives each page you visit a grade based on how aggressively it's trying to mine your data.

It's a good pick for getting maximum protection with minimal effort.

To keep you anonymized online, DuckDuckGo blocks tracking cookies that are able to identify you and your device, and even scans and ranks sites' privacy policies. You can clear tabs and data automatically at the end of each session, or you can wipe this data manually with a single tap. You can even set a timer to automatically clear out your history after a period of inactivity.

The browser extensions for Chrome and Firefox do a very similar job, so you don't have to abandon your favorite desktop browser to take advantage of DuckDuckGo's tight privacy controls. Again, the extensions rank sites for their privacy features, and block attempts to track your activities online.

What really appeals about the DuckDuckGo apps and browser extensions is how simple they are to use. You don't really need to do anything except install them, so it's a good pick for getting maximum protection with minimal effort.

Ghostery (Android, iOS, browser extension)

Get Ghostery for Android or iOS installed, and straight away it gets to work blocking adverts and tracking cookies that will attempt to keep tabs on what you're up to on the web.

Like DuckDuckGo's mobile apps, the Ghostery browser tells you exactly which trackers it's blocking, and how many monitoring tools each website has installed—if you find certain sites that are well-behaved, you can mark them as trusted with a tap.

Or, if you find a site that's packed full of tracking technology, you can block every single bit of cookie technology on it (for commenting systems, media players and so on), even if the site might break as a result.

Ghostery also develops an extension that works with just about every desktop browser out there—again, you can view the trackers on each site you visit, then take appropriate action on them or let Ghostery decide and its AI smarts decide what needs blocking.

Ghostery's tools are a little more in-depth and advanced than the ones offered by DuckDuckGo, so you might consider it if you want to take extra control over which trackers are blocked on which sites.

Tor Browser (Android, Windows, macOS)

Tor Browser stands for browsing "without tracking, surveillance, or censorship" and is worth a look if you want the ultimate in anonymized, tracker-free browsing—unless you're on iOS, where it isn't yet available.

The browser app for Android, Windows and macOS is actually part of a bigger project to keep internet browsing anonymous. The Tor Project routes your web navigation through a complex, encrypted network of relays managed by its community, making it much harder for anyone else to work out where you're going on the web.

As well as this additional layer of anonymity, Tor Browser is super-strict on the sort of background scripts and tracking technologies sites are allowed to run. It also blocks fingerprinting, a method where advertisers attempt to recognize the unique characteristics of your device across multiple sites, even if they can't tell exactly who you are.

See What's Next in Tech With the Fast Forward Newsletter

From artificial intelligence and self-driving cars to transformed cities and new startups, sign up for the latest news.

Your email

Enter your email

SUBMIT

By signing up you agree to our [User Agreement](#) (including the [class action waiver and arbitration provisions](#)), our [Privacy Policy & Cookie Statement](#) and to receive marketing and account-related emails from WIRED. You can unsubscribe at any time.

At the end of each browsing session, everything gets wiped, including cookies left behind by sites and the browsing history inside the Tor Browser app itself. In other words, private browsing mode is the default.

Because of the extra encryption and anonymity measures, Tor Browser can run slightly slower than other browsers, but in terms of staying invisible on the web, it's the best there is. It can even help you get online in countries where the internet is blocked or censored.

Brave ([Android](#), [iOS](#), [Windows](#), [macOS](#))

Brave is a project from Brendan Eich, once of Firefox developer Mozilla, and its mission includes both keeping you from being tracked on the web, and finding a better way to serve you advertisements. It's a dichotomy that doesn't fully fit together just yet.

There's no doubt about the effectiveness of its tracker blocking technologies, though. [The browser apps](#) block ads by default and put tight restrictions on the information sites can gather on you through cookies and tracking scripts.

You can block trackers, scripts, and fingerprinting technologies—where sites attempt to identify your particular device—individually, but unlike DuckDuckGo and Ghostery you don't get a detailed breakdown of what's been stopped.

Brave also tries to block phishing attempts over the web, and will force HTTPS encryption where it's available. It's a comprehensive package that strikes a well-judged balance between simplicity and power.

Time will tell whether Brave's attempts to create a new [privacy-respecting ad platform](#) are successful, but it's testing the idea of [paying users to watch ads](#) and splitting the revenue with content creators. You can also give micropayments to sites you like directly, though all of this is completely opt-in.

Firefox ([Android](#), [iOS](#), [Windows](#), [macOS](#))

As we mentioned at the outset, Firefox now blocks third-party cookies by default—those are the bits of code left by advertisers that try to piece together what you're doing across multiple sites to build up a more detailed picture of who

you are.

It also gives you a ton of information on each website you visit regarding the trackers and cookies that pages have attempted to leave, and which ones Firefox has blocked. Permissions for access to your location and microphone can be easily managed as well.

All this is on desktop—the mobile apps haven't quite caught up yet—but whichever platform you install Firefox on, you've got a raft of privacy-focused features to take advantage of. On mobile, you can again take control over tracker and cookie blocking, and clear out stored data every time you close down the app.

For even stricter tracker protection and ad blocking to boot, there's Firefox Focus for Android and iOS. It's a stripped-down version of the main browser, without all of the bells and whistles of the full Firefox, but if speed and privacy are your main priorities, it's definitely worth a try.

The main Firefox apps for desktop and mobile hit the sweet spot as far as balancing privacy and convenience. There's plenty to please those who want to take more control over how their data is collected, along with having all the usual browser features (like extensions and password syncing) as well.

Safari (iOS, macOS)

Apple continues to add anti-tracking tech to Safari with each successive release on iOS and macOS, though this isn't an option for your browser of choice if you're on Windows or Android of course.

Safari has already declared war on third-party tracking cookies that try and connect the dots on your web activity across multiple sites, and also blocks device fingerprinting techniques that try and identify you from the way your phone or laptop is configured.

Those protections are going to get tightened up even further with the arrival of iOS 13 and macOS Catalina in the fall. The browser will even warn you when you try and use a password that's too weak on a new website or service.

Safari also operates against the backdrop of Apple's commitment to collect as little information about you as possible and to keep most of that information locked away on your device rather than on Apple's servers.

Like most of Apple's products, Safari is an obvious choice if you use a lot of other Apple products in your daily life—you can jump seamlessly between browsing on an iPhone and a Mac, for example.

More Great WIRED Stories

- The Cold War project that pulled climate science from ice
- iPadOS isn't just a name. It's a new direction for Apple
- How to stop robocalls—or at least slow them down
- Everything you want—and need—to know about aliens
- How early-stage VCs decide where to invest
- 🦋 Want the best tools to get healthy? Check out our Gear team's picks for the best fitness trackers, running gear (including shoes and socks), and best headphones.
- 📧 Get even more of our inside scoops with our weekly Backchannel newsletter

One year for ~~\$29.99~~ \$10

Get WIRED

SUBSCRIBE

EXHIBIT 146

The Washington Post
Democracy Dies in Darkness

Help Desk: How to fight the spies in your Chrome browser

Our tech columnist answers your questions about how to protect your privacy while using Chrome, the most popular Web browser.

By Geoffrey A. Fowler

June 27, 2019 at 8:00 a.m. EDT

Is your Web browser spying on you? My recent column about the stark privacy differences between Google Chrome and Mozilla Firefox generated a lot of conversation — and questions from readers about what you can do to avoid surveillance while you surf.

The main lesson: If Google is a data vampire, Chrome is its fangs. For most people, not using a browser made by an advertising company is the simplest way to protect your data from thousands of tracking firms, including Google itself. I recommend switching to the nonprofit Firefox, which has privacy-focused default settings that automatically block tracking cookies from ad and data companies, including Google itself. Apple's Safari and Brave (which has an ad blocker built in) are also fine choices.

But I understand some people just can't quit Chrome. Barbara Karpel of Lauderhill, Fla., writes that her dental office uses software that asks for the Google browser. "When we submit a claim online, we are told that the insurance company's platform only accepts Chrome," she says.

Some people have invested in Chromebook laptops built around Google's browser — or just think Chrome is faster than the alternatives.

There *are* ways to defang Chrome, if you don't just use the default settings. Making Chrome better respect privacy requires messing around under the hood and installing privacy software, or extensions, into the browser.

Here's what I recommend to fight the advertising surveillance machine. Bonus: Some of these steps will also make websites load faster. Privacy for the win!

Don't count on Incognito mode to protect your privacy. Or a VPN.

First, a warning: The “private” browsing mode in Chrome probably doesn’t do what you think it does. Incognito is the privacy equivalent of using an umbrella in a hurricane. It keeps information from being saved on your computer’s search and browsing history, which is only useful if you want to hide your activity from other people who share your browser. It does not stop websites, search engines and Internet service providers from tracking what you do.

“Does using a VPN solve the privacy issues you spoke about on Google Chrome?” asks reader Dan Harmon. Unfortunately, no. A VPN, or virtual private network, can obscure what you do online from your Internet service provider, including your work, school or someone spying locally on your network. But if you’re logged into Google or Facebook, a VPN won’t stop the tech giants and their partners from tracking your searches and other things you do in Chrome.

Tell Google to collect less personal information

A great place to start is by telling Google itself to stop some of the tracking of your online activity that it associates with your Google account. I suggest checking two spots:

Log in to Google’s advertising settings (adssettings.google.com), and make sure “ad personalization” is set to “off.” Doing this will make Google stop targeting ads to you on sites such as YouTube, though it alone won’t stop Google from collecting data about you.

Then head over to your Activity controls (myaccount.google.com/activitycontrols) and turn off — or set to “pause,” in Google’s strange lingo — your “Web & App Activity.” This tells Google not to record your searches, ads you click on, apps you use and other data about how you use its services. The downside, as Google will remind you, is that some of its services might not work as well. While you’re in this menu, go ahead and also pause “Location History” as well as “Voice and Audio Activity.”

Make sure you’re not using Chrome Sync

In your Chrome browser, tap the circular icon in the top right corner to make sure you’re not signed in with your Google account and using the Sync function. This would allow Chrome to pass your browsing history to Google. (The data would be private if you also set a passphrase in Chrome, but most people haven’t done that.)

While you’re at it, tell Chrome not to automatically log in the browser to your Google account whenever you sign in to Gmail. To do that, tap the three dots in the upper right corner of Chrome to find your way to Settings. There, search “Gmail,” and you’ll find a setting for “Allow Chrome sign-in.” Set that to “off.”

There is one Chrome setting that privacy advocates disagree on: sending a “Do Not Track” request with your browsing traffic. Once upon a time, this was a good idea — but the industry hasn’t taken action on it, and now some data companies actually use it as one more way to track people. The argument for turning it on: You’re telling sites you specifically do not consent to them tracking you.

Add a privacy extension

You can download software to add to Chrome that works behind the scenes to automatically block tracking cookies and other snooping techniques used by an armada of ad and data companies.

These free programs work as extensions (also known as plug-ins) for the desktop version of Chrome. I have long used [Privacy Badger](#), which works with minimal hassle and is backed by a nonprofit that is squarely on our side, the Electronic Frontier Foundation. Other good choices include [DuckDuckGo](#) and [Disconnect](#), as well as [Ghostery](#) and [uBlock](#), which block both trackers and ads.

Blocking trackers is more of an art than a science, so don't be afraid to try a few of them to see which work best on the sites you use most often.

In addition to protecting your privacy, the extensions could help sites load faster because they scrape tracking code out of pages.

Protect Chromebooks, too

"I downloaded Firefox," writes Eva Hashemi from Boca Raton, Fla. "Then my son reminded me that his new laptop is a Chromebook. Yikes! Any advice on this? It's too late to return it."

All hope is not lost. If your Chromebook isn't locked down (say, by school administrators) and you can still add extensions, you could install the privacy software I recommended above.

Or another idea: If the version of Chrome OS you're using supports the installation of Android apps, then you could also install the Android version of Firefox via the Google Play store.

Stop using Google for searches

Asks John Peterson from Atlanta: "If I use [DuckDuckGo](#) as my default, is my privacy maintained when using my Mac installed with Chrome?"

Using a privacy-first search engine such as DuckDuckGo won't stop websites you visit from tracking you.

But changing your search engine to DuckDuckGo will definitely send less of your data to Google. Our searches are perhaps the most valuable personal information we share with Google — they convey not only what's on our minds, but also what we're looking to buy.

Chrome lets you switch your default search engine away from Google. Go to Settings, and then search for "search engine" and change the address bar setting.

DuckDuckGo is among the most well-known in the niche world of Google search alternatives. It promises not to track your searches or build a profile of you. It makes money through advertising around the context of what you search, rather than by tracking you.

Is it as good as Google? No. But it keeps getting better — and now claims over 41 million searches per day, up from 12 million in 2016. Clearly, interest in privacy is on the rise.

Read more tech advice and analysis from Geoffrey A. Fowler:

Don't smile for surveillance: Why airport face scans are a privacy trap

Not all iPhones are the same. These cost less and are better for the Earth.

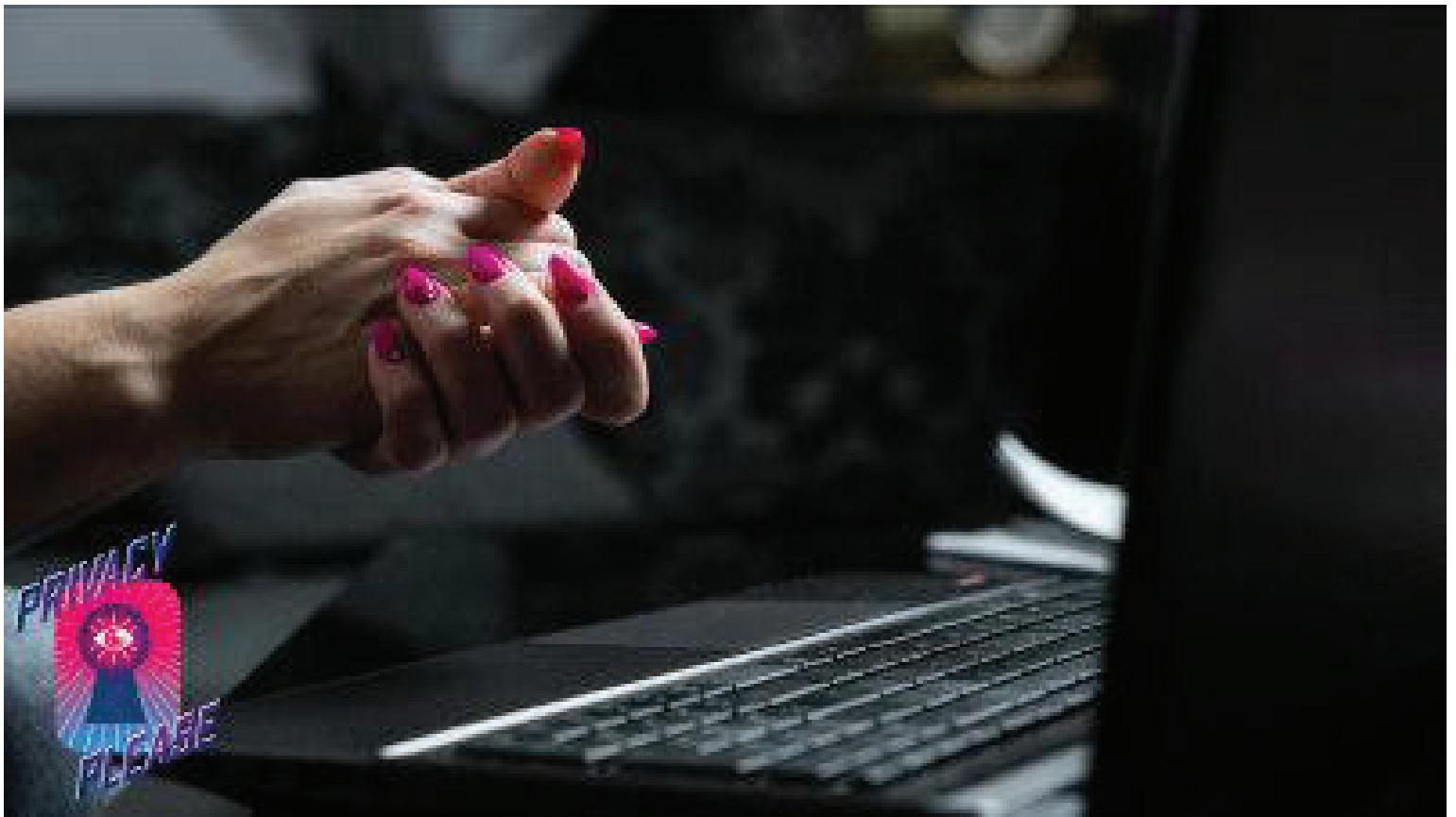
Rock this way: AirPods, Beats and Bose wireless ear buds take the headbang test

EXHIBIT 147

No, Incognito mode won't keep your porn habits private. This will.

A new study reveals that porn sites are leaking user data to third parties. Here's how to fight back.

By [Jack Morse](#) on July 18, 2019



Wipe it clean. Credit: SEBASTIAN GORCZOWSKI / GETTY

> Tech

[Privacy Please](#) is an ongoing series exploring the ways privacy is violated in the modern world, and what can be done about it.

Your dumb privacy tricks aren't working. They still know what kind of porn you're watching.

So concludes a [not-so-surprising study](#), which determined that online pornography sites are loaded with various trackers that leak private details about their users to third parties. And no, the study authors take pains to insist, **Google's Incognito mode won't keep your secrets.**

This latter point highlights broad confusion among the general public about what the Google Chrome feature actually does. **Many people believe it renders their online browsing private, when in reality it just prevents Chrome from "[saving] your browsing history, cookies and site data, or information entered in forms."**

Importantly, Google warns users, when using Incognito mode "[your] activity isn't hidden from websites you visit, your employer or school, or your internet service provider."

Which brings us back to porn. The study, conducted by researchers hailing from Microsoft, Carnegie Mellon University, and the University of Pennsylvania, found a significant majority of pornography websites — 93 percent of the 22,484 analyzed — "leak user data to a third party."

And it gets worse. "Our content analysis of the sample's domains indicated 44.97% of them expose or suggest a specific gender/sexual identity or interest likely to be linked to the user," continues the study.

In other words, your specific — and perhaps extremely private kinks — stand a pretty good chance of becoming not so private.

To illustrate this, the study authors lay out what for many is an all too familiar scenario.

"The websites [hypothetical porn consumer 'Jack'] visits, as well as any third-party trackers, may observe and record his online actions," explains the paper. "These third-parties may even infer Jack's sexual interests from the URLs of the sites he accesses. They might also use what they have decided about these interests for marketing or building a consumer profile."

Once companies have said profile on this unsuspecting porn consumer, continues the study, they "may even sell the data."

This is problematic for all kinds of reasons, in addition to the skeezy factor alone. If your porn consumption reveals sexual preferences that are banned or outright illegal in repressive countries, this sort of tracking could literally threaten your physical safety.

Thankfully, there is a way to watch porn anonymously online. It's called [Tor](#), and if it's not your [best friend](#) already, that should change today. Tor is an incredibly easy to use free service that keeps your identity private while browsing online.

There's even a Firefox-based [Tor browser](#), which means the only real technical skills you need to browse privately are the ability to download (and update) a browser.

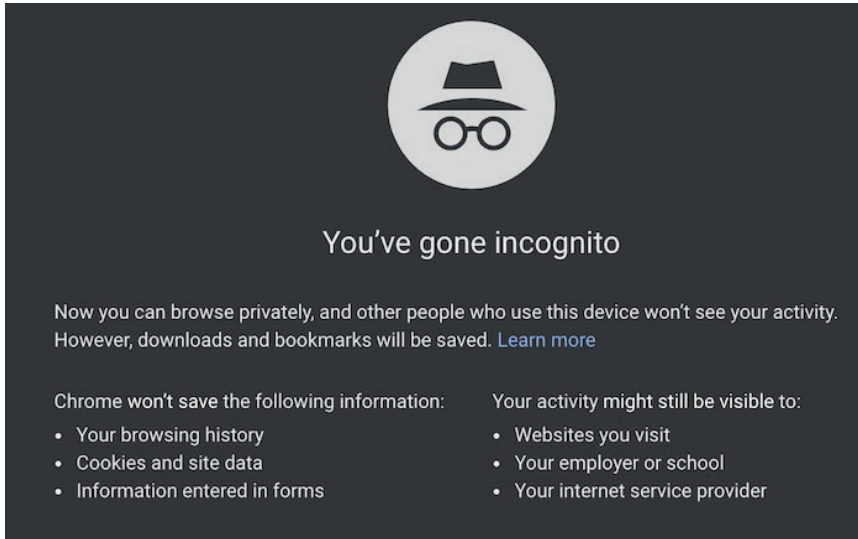
SEE ALSO: You should cover your phone's selfie camera, too

Oh, but there is one *tiny* catch: you can't go full-screen any more. That's right, it's only the default window-size setting for your porn viewing from now on. This small tradeoff is made necessary because of a type of tracking, known as [browser fingerprinting](#), that uses a computer's unique hardware and software settings to essentially fingerprint unique devices. Maximizing a browser window, which reveals some display features, helps in that process.

So there you have it: ditch the worthless Incognito mode, use Tor, and browse all that glorious internet porn to your heart's content. Hey, you can even use Tor for things *other* than viewing porn — after all, privacy is sexy.

EXHIBIT 148

MARK FRAUENFELDER 8:50 AM TUE DEC 3, 2019



Chrome's incognito mode is useful if you don't want your browsing history saved to your account, don't want websites to access your cookies, or if you want to troubleshoot your browser. But it doesn't do much to protect your privacy. Your ISP can see what websites you visit, and services like Twitter can figure out who you are even without cookies.

From [Tech Talks](#):

The easiest way for web applications to track users is to use cookies. But it is not the only way they can track you. Other bits of information can point to your device. For instance, I've seen some users use the Incognito window to browse Twitter, thinking that it will preserve their privacy and hide their identity. The premise is, since Incognito doesn't carry over their browser cookies, Twitter won't be able to associate their activity to their account.

But Twitter also keeps track of IP address, device type, device ID and browser type and version. Technically, it will be able to use all those factors to link your activity to your account. Facebook goes further and even tracks your activity across other websites when you're not logged in to your account.

TWEET COMMENTS

PRIVACY TIPS

EXHIBIT 149

Inc. 5000 Vision Conference Oct. 19-21 [Sign Up Now](#)



Inc.

NEWSLETTERS

SUBSCRIBE



TECHNOLOGY

Google Calls It Private Browsing. Oh, No It Isn't

It's such a tempting term, but please beware. There's very little that's private about it. [🔗](#)

BY CHRIS MATYSZCZYK, OWNER, HOWARD RAUCOUS LLC @CHRISMATYSZCZYK



Not so private? Getty Images

Absurdly Driven looks at the world of business with a skeptical eye and a firmly rooted tongue in cheek.

Humans are dreamers. That's why we get into so much trouble.

We dream of a perfect life and even when we get it, we realize it's not so perfect at all. Oddly, two Ferraris don't make us happier than one.

For many people these days, however, one significant dream revolves around privacy. We want to believe we're not being spied upon with every breath we take and every move we make. We want to believe we're clever enough to achieve that.

A temptation to that end is to open our laptops, launch a browser and go, as Google terms it, *Incognito*. With that name, Google encourages us to believe that we can potter about the web and no one will know:

Now you can browse privately, and other people who use this device won't see your activity.

How uplifting. You can do so many things without your beloved knowing. Like shopping for their gifts. Or, well, other things. Even Orwell would be impressed, right?

Well, except that if you read the smaller print fully -- and who does these days? --

Google is very clear just how private this form of browsing is:

First of all:

Downloads and bookmarks will be saved.

Then there's this:

Your activity might still be visible to: Websites you visit, your employer or school, your internet service provider.

Your employer? Your school? That really doesn't sound so good, does it? The truth is that private browsing is as private as our playing a video with the sound on at the airport.

It's always worth being careful in interpreting product names. The name *Incognito* implies that you can hide from prying eyes. The truth, though, is a little different. Or, indeed, entirely different.

It's not as if Google is alone in offering this kind of troubling misnomer. Firefox, for example, has so-called Private Windows. However, the non-profit explains:

Firefox clears your search and browsing history when you quit the app or close all Private Browsing tabs and windows. While this doesn't make you anonymous to websites or your internet service provider, it makes it easier to keep what you do online private from anyone else who uses this computer.

Easier. Relatively easy.

But in no way actually private.

Inc. helps entrepreneurs change the world. Get the advice you need to start, grow, and lead your business today. [Subscribe here](#) for unlimited access.

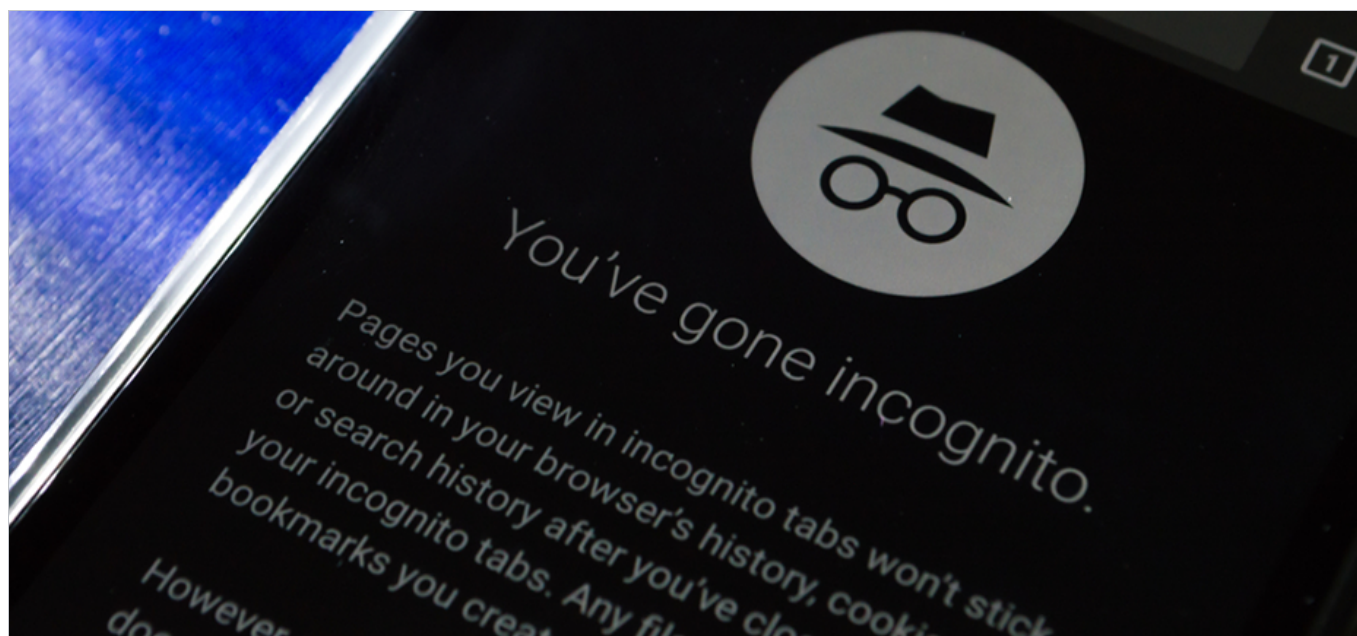
DEC 8, 2019

The opinions expressed here by Inc.com columnists are their own, not those of Inc.com.

EXHIBIT 150

How private is private browsing? Answer: only a little

DECEMBER 18TH, 2019



Maybe you're thinking: *I want privacy, so I'll just use my browser's "private browsing" feature, and I'm good to go.* If only it was so easy. Few technology features are surrounded by as many misconceptions as private browsing.

Private browsing features go by many names – for example, "Incognito Mode" in Google Chrome, and InPrivate in Microsoft Edge. Regardless of the name, they all work roughly the same way. They let you open a special browser window. While you're working inside that window, the browser won't store a local history of the pages you've browsed, the searches you've performed, or the forms you've filled out. Typically, it won't store cache files that it

would otherwise keep to help load sites faster when you return to them. Also, when you close a private browser session, your [browser will delete cookies \(" attr\(href\) "\)](#) created during that session – so if you return to a website where you'd logged in, the site won't recognize you, and you'll have to do it again.

Private browsing can help you keep your browsing history private from other individuals who might also have access to your computer. So, for example, it's handy if you're buying a gift for someone and you don't want them to know what it might be. Therefore, it's useful to know how to activate it:

In Google Chrome, press Ctrl+Shift+N, or click the menu button at the far right of the Chrome taskbar and choose New Incognito Window.

In Firefox, press Ctrl+Shift+P or click the menu button at the far right of the Firefox taskbar and choose New Private Window.

In Microsoft Edge, press the More Actions button [...] at the far right of the Edge taskbar and choose New InPrivate Window.

In Safari, press Command+Shift+N, or choose New Private Window from the File menu.

The limits of private browsing

But private browsing is *only* good for [protecting your online privacy \(" attr\(href\) "\)](#) from people you share your computer with. It won't safeguard your privacy on the internet. Here are five reasons why:

- 1 If you deliberately download a file or bookmark a page, your browser figures you want those, and it won't discard them. Your bookmark will be visible even in "non-private" mode.
- 2 It doesn't protect you on the network. So, if you open a private browsing session at work, and then visit sites you really shouldn't be visiting, it won't keep your employer from seeing what you're up to.
- 3 If you log in to Facebook or Google in private browsing mode, as long as you're logged in, they can track you just as they would ordinarily.
- 4 While private browsing might limit cookies, websites have [other ways to track you \(" attr\(href\) "\)](#) – for example, fingerprinting methods that recognize so many characteristics of your device that there's probably only one on earth with all of them: *yours*.
- 5 Private browsing does nothing at all to stop your internet service provider from tracking you.

If private browsing isn't private, what are your options?

So, what *can* you do if you want to browse privately? If you're running Safari (for Mac – not the Windows version), make sure "prevent cross-site tracking" is turned on. Safari also resists fingerprinting by trying to make your Mac look more like everyone else's. In Firefox, you can block many trackers, [cross-site tracking cookies \(" attr\(href\) "\)](#), and fingerprinters as follows: choose Options from the Firefox menu; choose Privacy & Security; and set Enhanced Tracking Protection to Strict.

All that said, the best way to limit most (but not all) tracking – including tracking by your internet service provider – is to subscribe to a Virtual Private Network (VPN) service you trust.

No matter where you go on the internet, you should [make sure you're protected \(" attr\(href\) "\)](#) by a strong security solution – there's always something trying to get to your information, so make sure your data is secure. Products like Sophos Home will keep your information safe wherever you go.

What are you waiting for? Let's get started!

[Free Download \(" attr\(href\) "\)](#)

No credit card required

[Buy Now - \\$59.99 \\$44.99 \(" attr\(href\) "\)](#)

EXHIBIT 151

Chrome Incognito mode – not as secure as you think

Panda Security

Whether you're looking for health information, or shopping for a surprise present for a loved one, there are times when you don't want your Internet browsing to be tracked. And this is where the Chrome Incognito browser mode is supposed to help.

Incognito does not mean what you think

According to the dictionary, incognito is an adjective that means "having one's true identity concealed". Or more simply, no one can tell who you are.

But when it comes to the Chrome web browser, **incognito mode is a lot less secretive than you would expect**. Despite claiming to allow you to browse in private, you can – and will – be identified as you surf the web using Incognito mode.

Advertisers know who you are

When you open an Incognito browser tab, Chrome displays a message, "Now you can browse privately, and other people who use this device won't see your activity." This would tend to suggest that no one can see what you are looking at.

But the reality is that Incognito offers **no protection at all from website operators and advertisers**. Anything you search will still be saved against your Google profile for instance. And various advertising trackers will continue to track you across the web, adding your "secret" activity to what they already know about you.

Advertisers know where you are

Advertisers also use a technology known as '[geolocation](#)' to figure out where you are. They use this information to show you ads for products and services in your local area, especially when using your mobile phone. But sometimes this can feel intrusive.

Again, **Incognito does nothing to hide location data**. So advertisers still know where you are – and they save that information to your advertising profile too.

Malware can still get through

Another common misconception is that browsing incognito protects your computer from malware and viruses. And again, this is completely untrue.

Incognito mode doesn't provide any additional security protections. If malware can install through your browser in "regular" mode, it will have no problem as you browse privately either. The only way to avoid virus infections is using a dedicated antimalware tool like [Panda Dome](#).

What is Incognito mode for?

At this point you're probably wondering what Chrome Incognito mode is actually for – but it does have one helpful function. Private browsing is designed to protect your privacy at home.

When browsing in normal mode, your browser records a complete history of every website you visit. It also collects various cookies and images that are stored on your computer to help make webpages load more quickly, or to remember passwords and logins. Anyone with access to your computer can use this information to reveal your secret browsing habits.

When surfing in Incognito mode, these cookies and temporary files are automatically removed; the web browsing history is also deleted when you close the browser. This prevents anyone being able to check up on what you have been doing on your computer.

So even though online advertisers know exactly what you've been looking at online, your partner's birthday present will still be a surprise – for them.

- [Privacy](#)
- [Safe Browsing](#)



Panda Security specializes in the development of endpoint security products and is part of the WatchGuard portfolio of IT security solutions. Initially focused on the development of antivirus software, the company has since expanded its line of business to advanced cyber-security services with technology for preventing cyber-crime.

EXHIBIT 152

cybernews.com

How private Google Chrome Incognito mode really is? | Cybernews

5-6 minutes

Google Chrome Incognito mode is a one-click solution for when you want to browse something privately. And indeed, once you close your incognito window, Chrome will forget everything about the session. This includes your browsing history, the given website permissions, the information you entered in forms, cookies, and site data.

All of this helps when you don't want other users who use the same computer to know where you've been. It also helps protect you from some forms of third-party tracking employed by websites.

However, the actual privacy benefits that you get from this mode are limited. Let's take a closer look at how well Chrome Incognito mode hides you. Spoiler alert: it's not that much.

How do you go incognito on Chrome?

You can activate incognito mode manually or via a keyboard shortcut. To do it manually:

- Press the three dot icon on the top-right corner of your browser
- Once the new window appears select New incognito window

If you want to use a shortcut instead, press **Ctrl + Shift + N** - this will instantly open an Incognito window.

Is Google Chrome Incognito safe?

Incognito mode offers a degree of privacy, but it's not a universal solution. Imagine that you're robbing a bank with a ski mask but no gloves. Sure, you're using partial protection required by your line of work, but it's not going to do much good when your fingerprints are all over the place.

It's the same with incognito mode, which only stops the browser from saving your browsing activity, cookies, passwords and the like to your local history. That means your IP address is still visible to the visited websites, whoever runs the network you're using, your internet service provider, and search engines. In short, it doesn't hurt, but it's far from the safety standard that you should be aiming for.

Why go incognito while browsing?

You might think, what are the uses of the Google Chrome Incognito mode, then? We've established that it doesn't help that much with privacy, but it still can be useful. Incognito mode is excellent for when you want to prevent something from entering your browsing history or don't want the browser to remember your log-in credentials. This is particularly useful when you want to log into your accounts, but many people use the same device.

Additionally, you can use multiple incognito window tabs to sign into different accounts. This way, they wouldn't override each other.

Also, as mentioned, some websites will have less ability to track you due to cookies being cleared on each subsequent visit.

How to browse privately

There are much better privacy solutions that could make your web browsing much safer. Here are some of the examples what you could do instead of relying on Incognito mode:

- Use a VPN to [mask your real IP address](#) and encrypt your connection. A [VPN](#) will route your connection through an intermediary server, making your activities invisible to your employees, school, and your internet service provider
- If possible, always use the encrypted HTTPS version of a website. Some extensions will force websites to load HTTPS instead of HTTP ([HTTPS Everywhere](#)). This makes your private information secure from hackers.
- Uninstall Flash and Java. With Java already out, and Flash set to end its life in 2020, there's no reason to keep these security holes on your browser.
- If you want to minimize tracking, use ad-blockers like Ghostery or uBlock Origin. They will combat intrusive code that tracks you across websites.
- Consider switching to more privacy-minded search engines like DuckDuckGo. It doesn't store your personal information and doesn't track you to serve ads.

FAQ

Can you be tracked in Incognito Mode?

Once you turn on the mode, you get a warning that your activity is still visible to websites, your employees or school, and your internet service provider. **So yes, you can still be tracked by your IP address**, which Google's Incognito Mode doesn't mask.

Does Incognito Mode save history?

When in Incognito Mode, the browser **won't save site data, cookies, browsing history, or information entered on forms by users**. It will still keep files that you download and bookmarks. It works the same way on desktop and mobile.

How to turn off Incognito Mode on Chrome?

You can quickly turn off Incognito Mode **by closing the tab**. The next time when you'll open a browser, you'll be browsing as though the session in Incognito Mode didn't happen.

How to disable Incognito Mode in Chrome Android?

If you need to turn off Incognito Mode on the mobile app, you'll need to press Switch tabs on the top right. On the right, you'll see your open Incognito tabs - close them. This will effectively end your private session.

EXHIBIT 153

What private browsing does—and doesn't—do to shield you from prying eyes online

Private browsing sounds like it's keeping all your browsing and data private—but its name is misleading.



[Photo: Pixabay/Pexels]

▼ MORE LIKE THIS

Microsoft Teams' new feature goes way beyond passive screen sharing

5 pieces of advice to help early stage founders navigate the months ahead

Bye, Zoom: This smart new app is the future of online meetings

BY LORRIE CRANOR AND HANA HABIB
4 MINUTE READ

Many people look for more privacy when they browse the web by using their browsers in privacy-protecting modes, called “Private Browsing” in Mozilla Firefox, Opera, and Apple Safari; “Incognito” in Google Chrome; and “InPrivate” in Microsoft Edge.

These private browsing tools sound reassuring, and they’re popular. According to a [2017 survey](#), nearly half of American internet users have tried a private browsing mode, and most who have tried it use it regularly.

However, [our research](#) has found that many people who use private browsing have misconceptions about what protection they’re gaining. A common misconception is that these browser modes allow you to browse the web anonymously, surfing the web without websites identifying you, and without your internet service provider or your employer knowing what websites you visit. The tools actually provide much more limited protections.

Other studies conducted by the [Pew Research Center](#) and the privacy-protective search engine company [DuckDuckGo](#) have similar findings. In fact, a [recent lawsuit against Google](#) alleges that internet users are not getting the privacy protection they expect when using Chrome’s

HOW IT WORKS

While the exact implementation varies from browser to browser, what private browsing modes have in common is that once you close your private browsing window, your browser no longer stores the websites you visited, cookies, user names, passwords, and information from forms you filled out during that private browsing session.

Essentially, each time you open a new private browsing window you are given a “clean slate” in the form of a brand-new browser window that has not stored any browsing history or cookies. When you close your private browsing window, the slate is wiped clean again and the browsing history and cookies from that private browsing session are deleted. However, if you bookmark a site or download a file while using private browsing mode, the bookmarks and file will remain on your system.

Although some browsers, including Safari and Firefox, offer some additional protection against web trackers, private browsing mode does not guarantee that your web activities cannot be linked back to you or your device. Notably, private browsing mode does not prevent websites from learning your internet address, and it does not prevent your employer, school, or internet service provider from seeing your web activities by tracking your IP address.

REASONS TO USE IT

We conducted a **research study** in which we identified reasons people use private browsing mode. Most study participants wanted to protect their browsing activities or personal data from other users of their devices. Private browsing is actually pretty effective for this purpose.

We found that people often used private browsing to visit websites or conduct searches that they did not want other users of their device to see, such as those that might be embarrassing or related to a surprise gift. In addition, private browsing is an easy way to log out of websites when borrowing someone else’s device—so long as you remember to close the window when you are done.

Private browsing provides some protection against cookie-based tracking. Since cookies from your private browsing session are not stored after you close your private browsing window, it’s less likely that you will see online advertising in the future related to the websites you visit while using private browsing.

Additionally, as long as you have not logged in to your Google account, any searches you make will not appear in your Google account history and will not affect future Google search results. Similarly, if you watch a video on YouTube or other service in private browsing, as long as you are not logged in to that service, your activity does not affect the recommendations you get in normal browsing mode.

WHAT IT DOESN’T DO

Private browsing does not make you anonymous online. Anyone who can see your internet traffic—your school or employer, your internet service provider, government agencies, people snooping on your public wireless connection—can see your browsing activity. Shielding that activity requires more sophisticated tools that use encryption, like virtual private networks.

Private browsing also offers few security protections. In particular, it does not prevent you from downloading a virus or malware to your device. Additionally, private browsing does not offer any additional protection for the transmission of your credit card or other personal information to a website when you fill out an online form.

It is also important to note that the longer you leave your private browsing window open, the more browsing data and cookies it accumulates, reducing your privacy protection. Therefore, you should get in the habit of closing your private browsing window frequently to wipe your slate clean.

WHAT’S IN A NAME

It is not all that surprising that people have misconceptions about how private browsing mode works; the word “private” suggests a lot more protection than these modes actually provide.

Furthermore, a **2018 research study** found that the disclosures shown on the landing pages of private browsing windows do little to dispel misconceptions that people have about these modes. Chrome provides more information about what is and is not protected than most of the other browsers, and Mozilla now links to an informational page on the **common myths** related to private browsing.

However, it may be difficult to dispel all of these myths without changing the name of the browsing mode and making it clear that private browsing stops your browser from keeping a record of your browsing activity, but it isn’t a comprehensive privacy shield.

EXHIBIT 154

Is Incognito Mode Actually Safe?

Nazli Ekim

Every day, millions of people use Google Chrome, which accounts for [67% of the worldwide browser market](#). Out of those millions of people, a fair portion use incognito mode in an attempt to maintain their privacy and stay safe on the web.

But incognito mode isn't as safe as you might think. While it does offer some minimal degree of privacy, it is in no way a shield against snoopers, nor is it an invisibility cloak. Even when using incognito mode, your browsing activity is still available to your internet service provider (ISP) and anyone else who has a bit of tech know-how.

Google Chrome isn't the only browser that offers incognito mode. Today, almost all browsers offer a similar feature, and all are similarly insecure. If you want to stay safe on the web, you need to take extra steps.

Here, we're going to cover what incognito mode and private browsing does, and what it doesn't do. Then, we'll provide some ways to actually keep yourself safe on the web.

What Incognito Mode Actually Does

When you switch on incognito mode (or Private Browsing in Firefox, etc.), what you're really doing is telling Chrome not to save your browsing history, cookies, and cache for the duration of your browsing session. Essentially, you're telling Chrome not to remember what you're about to do, but that doesn't mean that no one will save your information.

This can be very useful in protecting your data from other people with physical access to your computer, like family members and friends. For example, if you wanted to search for a surprise getaway for your spouse, it's a good idea to turn on incognito mode. That way, your past searches for "tickets to Honolulu" won't show up when your spouse hops on the computer and starts typing another search term that starts with the letter "t."

It's also extremely helpful for when you're borrowing someone else's computer or using a shared computer, like in a library, at work, etc. When you put on incognito mode before logging into a website, you can rest assured that your browsing data and login info won't be saved — by Chrome, that is. There's always the risk of keyloggers or other malware logging your information.

Plus, when you use incognito mode, you're not just telling Chrome not to save your new info, you're also telling it to temporarily forget your current history in the incognito window. This means that you can log into two separate accounts on the same website at once.

For example, you can log into Instagram in a regular Chrome window, and then open a new incognito window and log into a second account. Normally, you couldn't do this. But incognito mode essentially separates that window from your other browsing activity.

Additionally, you can use incognito mode when searching for airline tickets as some companies will change prices based on your search history. Since incognito mode "hides" your search history for the session, you can compare your incognito prices to your regular prices.

In short, incognito mode is useful when you don't want your browsing history or search history to be viewable by other people with physical access to your computer. It can also help when you need to log in to multiple accounts or check websites that may change based on your browsing history or cookies.

But if you actually want to stay safe and maintain your privacy online, you need to take additional security measures.

Get Keeper Unlimited & access all of your personal passwords on unlimited devices wherever you go!

[Buy Now](#)

What Incognito Mode Does Not Do

Incognito mode only prevents your data from being saved in Chrome (or another browser) on the computer you're using (assuming there aren't any keyloggers or other types of malware). It does not prevent other parties, like your ISP, websites, or cyber criminals using packet sniffing tools, from viewing what you're doing.

Think of it like this: imagine you're in a room with two other people, and you have a serum that makes someone forget everything they hear and do over the next two hours. You give one person the serum and tell them a secret. In two hours, they won't remember anything, so your secret's safe with them.

But wait — there was still another person in the room listening in on your conversation, and they didn't get the serum. Now, there's still someone out there who has your secret, and they can do whatever they want with it.

This is the problem with incognito mode: it will make Chrome forget what you tell it, but there are still other people in the metaphorical room with you. There's your ISP and the websites you visit, and if you're in a public place, there may also be cyber criminals using packet sniffing tools to view all the information you send.

All those other parties can still see what you're doing on Chrome without any issue. If you log into Facebook from an incognito tab, your ISP will know what you did, and Facebook will still have access to some of your data.

Even though your browsing history and cookies will be deleted once you close out of the incognito window, your data can still be traced back to you. These days, websites have access to sophisticated tools, like browser fingerprinting, that allow them to link your activity to your real identity even when you're using incognito mode.

Keep in mind that you need to be especially careful when you're using the internet at work or school. Many schools and companies have additional tracking software that allows them to see what you're doing, no matter whether you're using incognito mode or not.

For this reason, you shouldn't do anything you want to keep private on a work or school computer.

How Can I Actually Browse Privately?

Safe internet browsing is a bit of a rabbit hole — you can end up going pretty far down as there are very few ways to completely guarantee safety. Backdoors and vulnerabilities are being discovered every day, so there is always some risk every time you surf the web.

However, even though you can't totally eliminate the risk of crashing your car, you can still wear your seatbelt. When you're browsing the web, there are two things you can use to help you stay as safe as possible: using a VPN and a password manager.

A [VPN](#), or virtual private network, is a piece of software that obscures your IP address (think of it like your ID card) from your ISP and the websites you visit. When you fire up a VPN, your traffic is redirected through a secure, encrypted connection on a separate server. Essentially, your ISP will see that you've connected to a VPN, but everything after that will be private.

When you visit a website, your IP address will show up as your VPN's IP, not your own. This prevents websites from seeing who you are in most cases. Additionally, since your data is encrypted through the VPN, you can protect yourself from packet sniffers when using your computer on public WiFi.

Additionally, you can also use a password manager, like Keeper. Password managers allow you to securely store your passwords so you don't forget them. They can also generate strong passwords with the click of a button, save them securely, and quickly input them into websites with autofill. This means that you don't have to remember tons of long and complicated passwords, making it easy to avoid reusing the same, weak passwords over and over again.

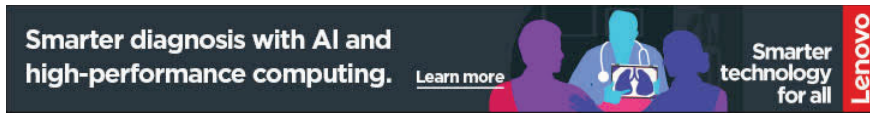
Conclusion

The internet is a treacherous place, and incognito mode doesn't do much to protect you. While it's useful for keeping your browsing history safe from friends, family, and coworkers, incognito mode doesn't prevent your data from being openly broadcast to the world wide web.

If you want to stay safe on the web, the best thing you can do is invest in a VPN and a password manager like Keeper. The combination of the two will keep your identity safe and greatly improve your password habits, which means your accounts will be much more difficult to breach.

Not a Keeper customer yet? [Sign up for a 30-day free trial now](#). Want to find out more about how Keeper Security can keep you safe on the web? [Reach out to our team today!](#)

EXHIBIT 155



Analytics Insight



INSIGHTS ▾

LATEST NEWS ▾

MAGAZINE ▾

INDUSTRY ▾

GEOGRAPHIES ▾

ABOUT US

PUBLISH ▾

CONNECT ▾

MORE +++ ▾

SUBSCRIBE

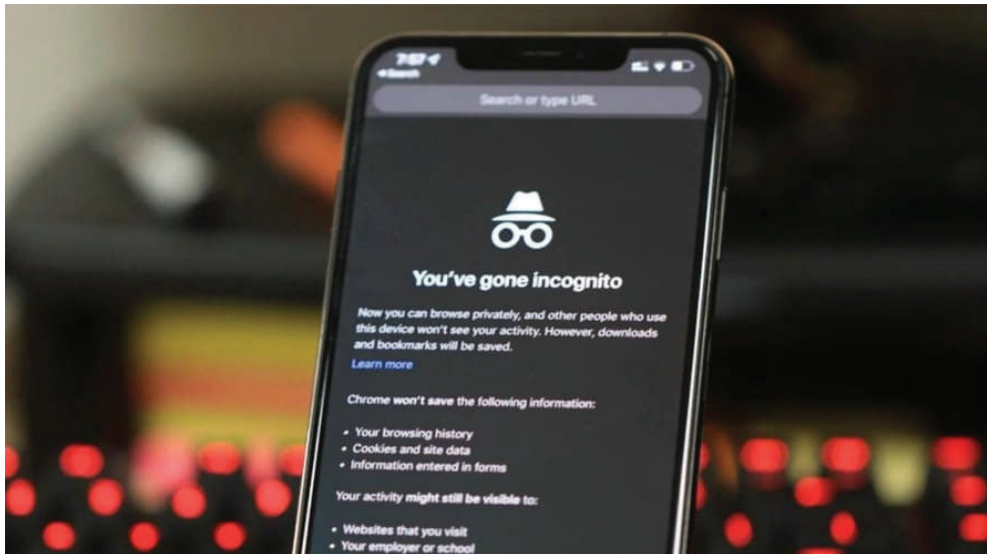
BOOST STARTUP



DON'T TRUST THE INCOGNITO MODE FOR ONLINE PRIVACY. DO THIS INSTEAD.

CYBERSECURITY LATEST NEWS

by Apoorva Komaraju / April 7, 2021

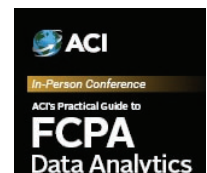


Even if you browse in Incognito mode, your data is being tracked.

For online privacy, if you've been trusting the incognito mode for browsing, think again. Google has been sued in California because it continues to track people's data even in the Chrome browser's incognito mode. Did that send a chill down your spine?

The name incognito has been etched in our minds in such a way that we instantly relate it to [complete data privacy](#), that anything you do online via the Chrome browser will not be tracked, but now we know that it's not all true. Even with the Incognito mode turned on, the Chrome browser will still permit websites and Google's own services to collect data about your surfing habits during that session. Not just that, the default search browser that most of us use, Google, also continues to track our online behavior, linking everything to our IP address.

MAGAZINES



Was this offensive on [Google's part](#)? Technically speaking, the company never claimed otherwise. When the Californian court refused to dismiss the case, Google told Bloomberg, "Incognito mode in Chrome gives you the choice to browse the internet without the activity being saved to your browser or device. As we clearly state each time you open a new incognito tab, websites might be able to collect information about your browsing activity during your session."

Is There An Alternative To Chrome's Incognito Mode?

Vivaldi is a web browser that's built on the same Google Chrome engine and has all its extensions too, but with stronger privacy. Vivaldi's equivalent of the Incognito mode is their Private Window. The default search engine in Vivaldi is DuckDuckGo, the search engine that is known for [not collecting any personal information about its users](#). Vivaldi also makes sure that it stops any trace of your web activity from being left behind on the computer. It minimizes whatever is stored on the disk other than relying on the computer's memory to store critical information, to ensure that there is not even the slightest trail of your activities being discovered later.

[Talking about online privacy](#), Vivaldi has many [privacy protections inbuilt](#). If you explore the Vivaldi settings, for example, under the privacy tab you will find the option to block the trackers and ads in any session. The search suggestion option, that tries to predict what you are searching for is also turned off by default for online privacy reasons. Unlike Google, Vivaldi does not store information like bookmarks or history. Even if you are using Vivaldi browsers on different devices, it will encrypt the information. [This offers greater privacy](#).

There's Also A Way To Protect Your Privacy On Chrome

If you want to stick with Chrome as your default browser, this is what you can do. DNS over HTTPS will mask the websites you visit from your internet provider and anyone who is trying to track your information. To turn on this feature, go to Chrome's settings and search for DNS and find the secure DNS feature. Select a provider from the "with" dropdown window and ensure to select the option "with".

Firefox also has this feature in its settings.

Join Our Telegram Channel for More Insights. [JOIN NOW](#)



Executive
Development

PROFESSIONAL

Data Science & Analytics
for Strategic Decisions

2 MONTHS, ONLINE | STARTS 15 DEC 2021

APPLY NOW

[ONLINE PRIVACY](#)

SHARE THIS ARTICLE

DO THE SHARING THINGY



December 3, 2021
Gaylord National Resort
& Convention Center
Washington, DC

**The *Only* Event
of its Kind!**

Join, Network and
Benchmark with:

Pfizer
Google
Zimmer Biomet
Panasonic
ABInBev
HSBC
Amgen
Cargill
And More!

[LEARN MORE](#)

MOST POPULAR



[ARTIFICIAL INTELLIGENCE LA
LATEST NEWS](#)

Top 20 B.Tech in Artificial
Intelligence Institutes
[August 27, 2019](#)



[ARTIFICIAL INTELLIGENCE LA
REGION TOP LIST UNCATEGORIZED](#)

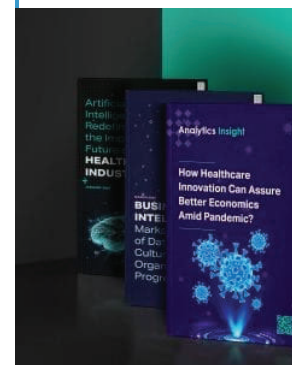
Top 10 Countries Lead
Artificial Intelligence R
[June 27, 2019](#)



[ARTIFICIAL INTELLIGENCE LA
ROBOTICS TOP LIST](#)

Top 10 Robotics Comp
the World
[February 6, 2018](#)

E-BOOKS



PRESS RELEASES

ABOUT AUTHOR

MORE INFO ABOUT AUTHOR



Apoorva Komaraju

[More by Apoorva Komaraju »](#)

RELATED LATEST NEWS ARTICLES

SIMILAR POSTS FROM LATEST NEWS CATEGORY



Augmented Analytics is the Tomorrow of Business Intelligence
November 5, 2018



Applications of Natural Language Processing in Different Sectors
October 23, 2020



Driving Business Intelligence Through Web Data Mining
September 23, 2020



LATEST NEWS PRESS RELEASES

Singapore based crypt Coinstore enters India Coinstore allocates US\$ for India expansion and

November 29, 2021



ARTIFICIAL INTELLIGENCE LA PRESS RELEASE

Prevision.io Launches I As-You-Go AI Management Platform to Make AI Accessible to All Companies

Prevision.io has launched of-its-kind AI Management Platform on Google

November 22, 2021



LATEST NEWS PRESS RELEASES

Dell Technologies Delivers to Autonomous Operation CloudIQ

Leverage autonomous in collaboration with Dell Technologies and Cloud

November 17, 2021





ABOUT US



Analytics Insight

Analytics Insight® is an influential platform dedicated to insights, trends, and opinion from the world of data-driven technologies. It monitors developments, recognition, and achievements made by Artificial Intelligence, Big Data and Analytics companies across the globe.



Select Language:



LINKS

About AI

Know Us
Privacy
Policy
Media Kit
Content
Licensing
Terms &
Conditions

Reach Us

Contact
Advertise
Publish
Interview
Careers
Sitemap

Special Editions

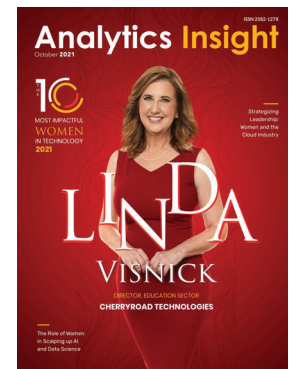
40 Under 40 Innovators
Women in Tech
Top 100
Market Reports
AI Glossary
Podcast
Infographics

Sign up Now

Get AI newsletter delivered to your inbox, and more info about our products and services

NEWSLETTER

LATEST ISSUE



SUBSCRIBE

EXHIBIT 156

CNN

▲

AudioLive TV

MARKETS

see all →

▲ **DOW** 32,845.13 +315.50 +0.97%

▲ **S&P 500** 4,130.29 +57.86 +1.42%

▲ **NASDAQ** 12,390.69 +228.09 +1.88%

FEATURED

[Crypto 101](#)

Crypto 101

Everything you need to know about bitcoin, blockchain, NFTs and more

LATEST

Instagram walks back updates after criticism from Kardashian family

Tesla, GM buyers would get EV tax credits again under Democrats' climate bill

Treasury Secretary Janet Yellen: US economy remains 'resilient' despite GDP decline

Private browsing may not protect you as much as you think

By Jennifer Korn, CNN Business
Updated 8:31 AM EDT, Mon July 25, 2022

See More Videos

New York (CNN Business) — For years, the most popular internet browsers have included options to search for and visit websites in “private” modes. Those options may now be viewed as vital tools for some in the wake of *Roe v. Wade*’s demise, as abortion-seekers look to avoid having their personal data used against them in states where abortion is criminalized.

But clicking the “private” browsing option might not protect you as much as you think, some privacy experts say.

These options have different names — Private Browsing on Safari and Firefox, and Incognito mode on Chrome — but the functionality is similar on each. In these private modes, the chosen browser does not keep a log of sites visited, cached pages, or saved information like credit card numbers and addresses. It also prevents information from sessions from being stored in the cloud.



RELATED ARTICLE

Search histories, location data, text messages: How personal data could be used to enforce anti-abortion laws

Although using these options does add a certain level of protection online, privacy experts say it stops short of preventing the user from being tracked altogether – potentially limiting the protections it may afford women in this new legal landscape.

“We have to recognize that oftentimes simply toggling on a private mode does very little to prevent third-party tracking and especially law enforcement tracking,” said Albert Fox Cahn, founder and executive director of the Surveillance Technology Oversight Project and a fellow at the New York University School of Law.

What does private browser mode do?

As designed, private browsing modes are best suited for protecting your web activity from other people who use the same device, according to experts, but it does little beyond offering that local shield.

“It can be helpful, for example, for trans and queer kids who are worried about being tracked by their parents and for people who may be in a situation where they can’t securely separate their computer from other people who can access the browser history,” says Fox Cahn.

The private mode can also help reduce tracking across websites. On Chrome, for example, users are told: “Websites see you as a new user and won’t know who you are, as long as you don’t sign in.”

“People choose to browse the web privately for many reasons,” said Parisa Tabriz, VP of Chrome Browser. “Some people wish to protect their privacy on shared or borrowed devices, or to exclude certain activities from their browsing histories. Incognito helps with these use cases.”



RELATED ARTICLE

Period-tracking apps are trying to make women feel safer about their data after the end of Roe v. Wade

Usually when a person browses online, companies will use tracking devices known as cookies to keep up with digital activity from one site to the next for better targeted advertising. Depending on the browser and user choices, private browsing mode can reduce that cross-site information sharing. But with some browsers, users must know to select these additional options, beyond simply opting for private mode.

Safari, for example, has a default Intelligent Tracking Prevention feature, which limits cross site tracking while enabling sites to continue to function normally. Its “Prevent Cross-Site Tracking” and “Block all cookies” options are extra steps to protect users, but these features are separate from private mode. Chrome, meanwhile, advises users that they have to choose to block third-party cookies, even in Incognito mode. Firefox added new default features last year, including “total cookie protection,” to stop users from being tracked around the internet, as well as “smart block” to allow for third-party logins through sites like Facebook or Twitter while still working to prevent tracking.

You give us five minutes, we'll give you five things you must know for the day.

By subscribing you agree to our [privacy policy](#).

Private modes are also limited in their effectiveness when it comes to IP addresses, which tie to the device and can be used to geo-locate the user.

“Whether you’re in privacy mode or not, your IP address always has to be known by the recipient because when your browser sends the request to get data, the server that’s receiving the request needs to know where to send that data back to,” said Andrew Reifers, associate teaching professor at the University of Washington Information School. An internet service provider can also record a user’s online activity regardless of their browser privacy setting.

Some browsers do offer additional protections to address this. Safari has a “Hide IP Address” selection separate from private browsing mode that, when enabled, sends user browser information to two different entities, with one getting the IP address but not the website being visited and the other getting the website but not IP address. In this way, neither has all the information on a user. Other browsers also have options to mask IP addresses, such as VPN extensions or “disable Geo IP” capabilities that stop browsers from sharing a user’s location with websites.

What do private browser modes not protect?

Online browsing is stored in two places: on the local computer and by the sites visited. When a user in private browsing mode goes to Facebook, for example, there will not be a stored record of that visit on their device, but there will be a stored record of that visit in their Facebook account records and by Facebook's ad analytics.

The record users leave online, with or without enabling private browsing options, creates much uncertainty around how that data could be used as evidence by law enforcement in states that criminalize abortions. Tech companies have said little about how they would handle such requests. Groups promoting digital rights and reproductive freedoms are now warning people in these states to safeguard their digital footprints when seeking abortion information and resources online, and sharing tips for how to do so.



RELATED ARTICLE

HHS issues new guidance on post-Roe v. Wade patient privacy

Moreover, if someone is working on a company or school-owned laptop, private browsing mode won't do much at all. "If you have a computer where somebody else is managing it, having privacy against that person is not really possible," said Eric Rescorla, CTO at Mozilla. "If an employer owns your computer, they can put any kind of monitoring software on the computer they want, and they can measure anything that you do. So, no, it doesn't protect you against that, but almost nothing would."

Google Chrome also warns users that Incognito Mode cannot offer total protection in these cases. "When in Incognito Mode, your activity might still be visible to websites you visit, your employer or school, or your internet service provider. We make this clear when opening Incognito Mode," said Tabriz.

Users should also keep in mind that the protections offered in private mode are exclusive to web browsing, leaving any activity on smartphone apps vulnerable. No matter how well private browsing mode works to protect user activity, it can't help anywhere else. "A lot of the applications that we use don't have a built-in incognito mode," said Reifers. "You don't really know what that application is storing."

What extra steps can you take to protect yourself online?

Beyond enabling private browsing modes, and selecting the additional privacy options offered by the companies in their settings, there are some additional steps users can take to try to maximize digital privacy,

A VPN, or virtual private network, conceals an IP address to make a user more anonymous online, effectively protecting both who and where a user is. "A good first step would be to use a private browsing mode and a VPN together," Rescorla said.

But using a VPN potentially allows the VPN operator access to your browsing activity. "Many of these will sell that information or certainly make it available to police if they provide a warrant," warns Fox Cahn.



RELATED ARTICLE

Alphabet CEO Pichai can be questioned in privacy lawsuit, judge rules

Internet users can also consider turning to a browser like Tor, a secure and anonymous option that uses multiple intermediary servers to keep any single server from fully tracking activity, according to privacy experts.

Above all, experts stress that internet users should be aware that online activity is fundamentally just not private, regardless of browser setting. And while clearing browsing history and emptying cookie caches make data recovery harder for third parties, it is still not impossible with certain forensic tools and warrants.

Fox Cahn emphasizes that those concerned with data privacy like abortion seekers should take as many steps as possible, even buying a new device that is not traceable or using services like Tor. "It's cumbersome, but that provides a lot more protection," he said. "You have to keep in mind that all these things can do is reduce the amount of risk. None of them are absolutely perfect."

MORE FROM CNN BUSINESS



Electric truck maker Rivian laying off 6% of its workforce



FTC files to block Facebook-parent Meta from buying a VR company

CNN BUSINESS VIDEOS



Is the US in a recession? Hear what Jerome Powell thinks



See CNN's coverage of the first crew on the International Space Station in 2000



BlackRock investment expert: Fed will start slowing interest rate hikes



FULL SHOW 07/27/2022: The Fed's battle against inflation



CONTENT BY THE ASCENT

You can now avoid credit card interest until 2024

A slam dunk if you need a balance transfer (21 months)

It's official: now avoid credit card interest into 2024

0% intro APR until 2024 is 100% insane

Leading cash back card now has 0% intro APR until nearly 2024

Paid Links



Search CNN...



Log In

Live TV

Audio

World

US Politics

Business

Health

Entertainment

Tech

Style

Travel

Sports

Videos

Features

Weather

More



FOLLOW CNN BUSINESS



Most stock quote data provided by BATS. Market indices are shown in real time, except for the DJIA, which is delayed by two minutes. All times are ET. Disclaimer. Morningstar: Copyright 2018 Morningstar, Inc. All Rights Reserved. Factset: FactSet Research Systems Inc.2018. All rights reserved. Chicago Mercantile Association: Certain market data is the property of Chicago Mercantile Exchange Inc. and its licensors. All rights reserved. Dow Jones: The Dow Jones branded indices are proprietary to and are calculated, distributed and marketed by DJI Opco, a subsidiary of S&P Dow Jones Indices LLC and have been licensed for use to S&P Opco, LLC and CNN. Standard & Poor's and S&P are registered trademarks of Standard & Poor's Financial Services LLC and Dow Jones is a registered trademark of Dow Jones Trademark Holdings LLC. All content of the Dow Jones branded indices Copyright S&P Dow Jones Indices LLC 2018 and/or its affiliates.

[Terms of Use](#) [Privacy Policy](#) [Do Not Sell My Personal Information](#) [Ad Choices](#) [Accessibility & CC](#) [About](#) [Newsletters](#) [Transcripts](#)

© 2022 Cable News Network. A Warner Bros. Discovery Company. All Rights Reserved.

CNN Sans ™ & © 2016 Cable News Network.

